高等学校计算机应用规划教材

计算机网络安全教程

◆ 网络协议及网络安全基础
◆ 计算机物理安全
◆ 操作系统安全
◆ 密码学基础
◆ 身份认证与访问控制
◆ 数据库安全
◆ 恶意软件概念及防范
◆ Internet安全协议
◆ 公钥基础设施——PKI
◆ 网络安全技术
◆ 无线网络安全技术
◆ 数据备份
◆ 信息安全评测与风险评估
◆ 计算机网络安全管理



石 勇　卢 浩　黄继军　编著

清华大学出版社

高等学校计算机应用规划教材

计算机网络安全教程

石 勇 卢 浩 黄继军 编著

清华大学出版社

北 京

内 容 简 介

本书从网络安全的理论基础着手，同时兼顾实际工作中的应用，深入浅出地介绍了网络协议的基础知识、网络安全基础、计算机物理安全、操作系统安全基础、密码学基础、身份认证与访问控制、数据库安全、恶意软件概念及防范、Internet 安全协议、公钥基础设施——PKI、网络安全技术、无线网络安全技术、网络应用安全、数据备份、信息安全评测与风险评估和计算机网络安全管理等内容，书中通过大量实例、图文并茂的说明，使读者能在最短的时间内理解消化相关知识，并能学以致用，每章结尾均配有课后习题供读者练习巩固。按照本书的内容，逐步学习，并加以实践操作，即可掌握相关的技术内容。

本书可作为高等学校计算机网络安全课程的教材，也可供广大网络管理员参考。

图书在版编目(CIP)数据

中国版本图书馆 CIP 数据核字(2011)第号

责任编辑：刘金喜　胡花蕾
装帧设计：孔祥丰
责任校对：蔡　娟
责任印制：
出版发行：清华大学出版社
http://www.tup.com.cn
地　　址：北京清华大学学研大厦 A 座
邮　　编：100084
社　总　机：010-62770175
邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　**印　　张：**21.75　**字　　数：**543 千字
版　　次：2012 年 1 月第 1 版　**印　　次：**2012 年 1 月第 1 次印刷
印　　数：1～4000
定　　价：35.00 元

产品编号：

前　　言

计算机网络已逐步深入应用到政治、经济、军事等各个领域，以及人们工作和生活的方方面面，给国家、社会带来了巨大影响和深远变革，伴随而来的网络安全问题也逐步引起了人们的高度关注。

计算机网络安全保障是一项系统工程，包含诸多复杂的环节，任何一个环节的缺陷或问题，都会摧毁整个系统的安全防线。网络安全保障，需要从物理(实体)安全、运行安全、数据(信息)安全、管理(人员)安全几个方面全面着手。

本书共分为 16 章，编写时采用先理论分析为主，后侧重实践应用的思路。

第 1 章介绍了 TCP/IP 协议的基础知识，包括 TCP/IP 协议体系及其各层协议的主要功能、主要概念。

第 2 章介绍了网络安全的基础知识，包括网络安全的发展历程、安全威胁、安全需求分析、安全模型。

第 3 章介绍了物理安全，包括环境安全、机房安全、设备安全、突发事件应急计划。

第 4 章讲述了操作系统安全，包括 Windows 系统安全、Linux/UNIX 系统安全、操作系统漏洞、操作系统入侵检测等内容。

第 5 章介绍了密码学基础知识，包括密码学的基本概念、对称密码算法、非对称密码算法、散列函数、数字签名等。

第 6 章阐述了身份认证与访问控制机制，包括身份认证与访问控制的基本概念、类型等内容。

第 7 章介绍了数据库安全相关内容，包括数据库安全特性、数据库安全威胁、数据库数据保护、数据库备份与恢复，以及 SQL Server 数据库安全机制。

第 8 章介绍了恶意软件概念及防范，包括恶意软件的分类和各类恶意软件的特征、运行症状、防范方法。

第 9 章介绍了网络安全相关的 IPSec、TLS、Kerberos、SET 等安全协议。

第 10 章介绍了 PKI(公钥基础设施)，包括其概念、功能、组成、信任模型、相关标准等。

第 11 章介绍了网络安全相关的技术，包括防火墙、入侵检测、VPN 等。

第 12 章阐述了移动通信网络与无线局域网的安全性分析及安全防护。

第 13 章介绍了应用安全，包括口令安全、网络监听、网络扫描、钓鱼攻击、Web 安全等。

第 14 章介绍了数据库备份相关的数据存储技术、远程数据备份、个人数据备份。

第 15 章介绍了信息安全评测与风险评估。

第 16 章介绍了计算机网络安全管理相关原则、标准、法规。

本书通过大量的实例，力图避免网络协议、网络安全相关书籍枯燥抽象的通病，使读者能在最短的时间内学以致用。书中各章不仅详细介绍了实例的具体操作步骤，而且还配有一定数量的练习题供读者学习使用。读者只需按照书中介绍的步骤一步步地实际操作，就能完全掌握本书的内容。

本书可作为高等学校计算机网络安全课程的教材，也可供广大网络管理员参考。

本书编写人员分工如下：石勇编写第 1～5 章，卢浩编写第 6～8 章，黄继军编写第 9～11 章，程凤娟编写第 12～16 章。此外，苏兆锋、王雷、许云、苏小平、刘兰、王梅、张宏、孙浩、杨彬、关涛、苏玉林、于文杰等也参与了本书的编写和修改，在此向他们致以诚挚的谢意！

编者力图使本书的知识性和实用性相得益彰，但由于水平有限，书中错误、纰漏之处难免，欢迎广大读者、同仁批评斧正。

编　者

2011 年 4 月

目　　录

第1章　网络协议基础

信息革命是继农业革命、工业革命之后，人类历史上的第三次革命，它对整个人类社会及生活产生了深远的影响，目前，这种影响还在以超乎想象的速度持续进行着。

计算机网络是信息技术存在与发展的基石，是通信技术与计算机技术结合的产物。计算机网络利用通信设备和线路，将地理位置不同、功能独立的多个计算机系统相互连接起来，通过网络协议来实现信息传递和资源共享。

高速发展的信息技术，在大幅提高工作效率、提供种种生活便利的同时，也带来了日益严重的安全隐患。电影《虎胆龙威4》中利用计算机网络操纵国家基础设施进行犯罪的情节，绝非危言耸听。事实上，各行各业在信息化进程中，最容易被忽视，出现问题后最难挽回、弥补的一个环节，就是信息安全的保障。信息安全保障涉及多个方面，其中，计算机网络的复杂性、普通用户的低安全防范意识和低安全防范水平，使得计算机网络安全问题尤为突出。

要准确把握计算机网络安全的内涵，掌握计算机网络协议是其基本要求。理解计算机网络协议的基本运行原理，才能掌握看似简单的网络操作背后蕴含的多个环节，才能考察各个环节是否安全，才可能设法保障网络安全。计算机网络安全保障遵循“木桶原理”，一个环节出现问题，整个网络的安全都无从谈起。所以，对网络协议的全面领会，是保障计算机网络安全的基础。

通常，学习网络协议是一个枯燥乏味、令人生厌的过程，很容易让人感觉过于抽象，晦涩难懂，其实这是一个误解。事实上，网络协议时刻体现在每一个细微的网络操作中，本章将通过大量的实践案例，将网络协议的运行过程向读者展现出来，力图使网络协议的学习过程不再枯燥抽象、高深莫测。

本章重点

- TCP/IP 参考模型
- 数据在各层协议间的流动
- 链路层协议的主要功能、以太网、帧的概念
- 网络层协议的主要功能、主机端到端传输概念
- 传输层协议的主要功能、应用程序端到端传输概念
- 应用层 DNS、HTTP、FTP、SMTP、POP3 协议的基本概念

1.1　网络发展概述

根据中国互联网络信息中心(CNNIC)在北京发布的《第 25 次中国互联网络发展状况统计报告》，截至 2009 年 12 月，我国网民规模已达 3.84 亿，网络出口带宽达到 866Gb/s，距 1986 年中科院高能物理研究所首度与 Internet 建立电子邮件连接仅 20 余年时间。计算机网络的迅猛发展，以不可逆转的趋势影响着我们工作和生活的方方面面。

计算机网络的发展，经历了联机系统、计算机互联网络、标准化网络、网络互联与高速网络四个阶段。

联机系统，即以一台中央主计算机连接大量地理上处于分散位置的终端。终端通常指一台计算机的外部设备，包括显示器和键盘，无中央处理器。这一阶段可追溯到 20 世纪 50 年代。那时人们开始将彼此独立发展的计算机技术与通信技术结合起来，完成了数据通信与计算机通信网络的研究，为计算机网络的出现做好了技术准备，奠定了理论基础。

从 20 世纪 60 年代中期开始，出现了若干个计算机互联的系统，开创了计算机——计算机通信时代。随后各大计算机公司都陆续推出了自己的网络体系结构，以及实现这些网络体系结构的软、硬件产品。1974 年 IBM 公司提出的 SNA(System Network Architecture)和 1975 年 DEC 公司推出的 DNA(Digital Network Architecture)就是两个著名的例子。这种自成体系的系统被称为封闭系统，各厂家提供的网络产品实现互联十分困难，人们迫切希望建立统一的国际标准，渴望得到一个开放的系统。

20 世纪 70 年代中期，计算机网络开始向体系结构标准化的方向发展。1984 年国际标准化组织(International Organization for Standaradization，ISO)正式颁布了开放系统互联参考模型(Open System Interconnection，OSI)，简称为 ISO/OSI 七层参考模型。20 世纪 80 年代，美国电气与电子工程师协会(Institute of Electrical and Electronics Engineers，IEEE)为了适应微型计算机、个人计算机(PC)以及局域网发展的需要，于 1980 年 2 月在旧金山成立了 IEEE 802 局域网标准委员会，并制定了一系列局域网标准。在此期间，各种局域网大量涌现。新一代光纤局域网——光纤分布式数据接口(Fiber Distributed Data Interface，FDDI)网络标准及产品也相继问世。这一阶段典型的标准化网络结构如图 1-1 所示，通信子网的交换设备主要是路由器和交换机。通信子网之外的部分由各种类型的大量主机构成，信息资源存放于这些主机中，故通常称此部分为资源子网。

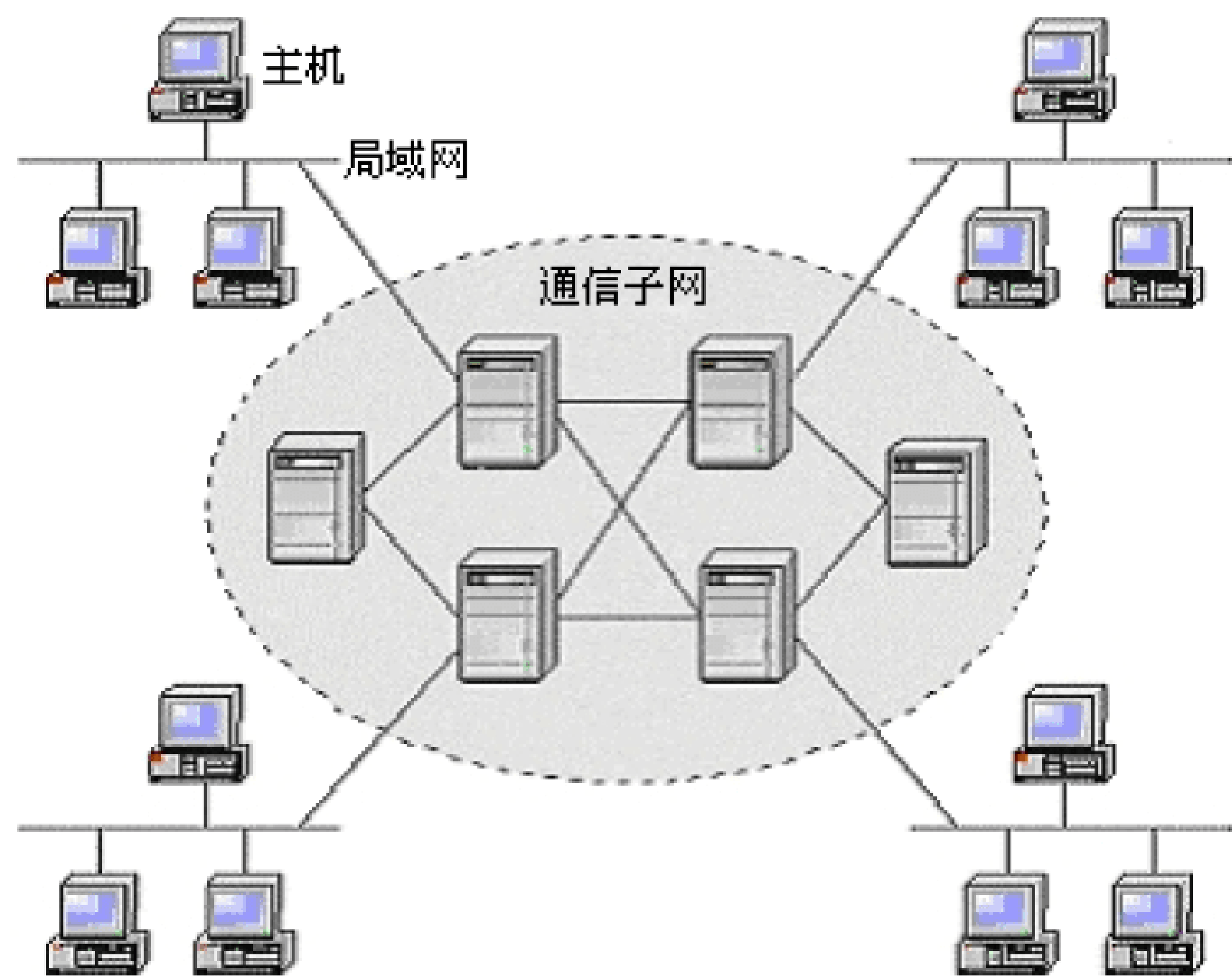


图 1-1　标准化网络

进入 20 世纪 90 年代，随着计算机网络技术的迅猛发展。特别是 1993 年美国宣布建立国家信息基础设施(National Information Infrastructure，NII)后，全世界许多国家都纷纷规划建设本国的NII，从而极大地推动了计算机网络技术的发展，这样计算机网络的发展进入一个崭新的阶段，这就是计算机网络互联与高速网络阶段。目前，全球以 Internet 为核心的高速计算机互联网络已经形成，Internet 已经成为人类最重要的、最大的知识宝库。网络互联和高速网络被称为第四代计算机网络，如图 1-2 所示。

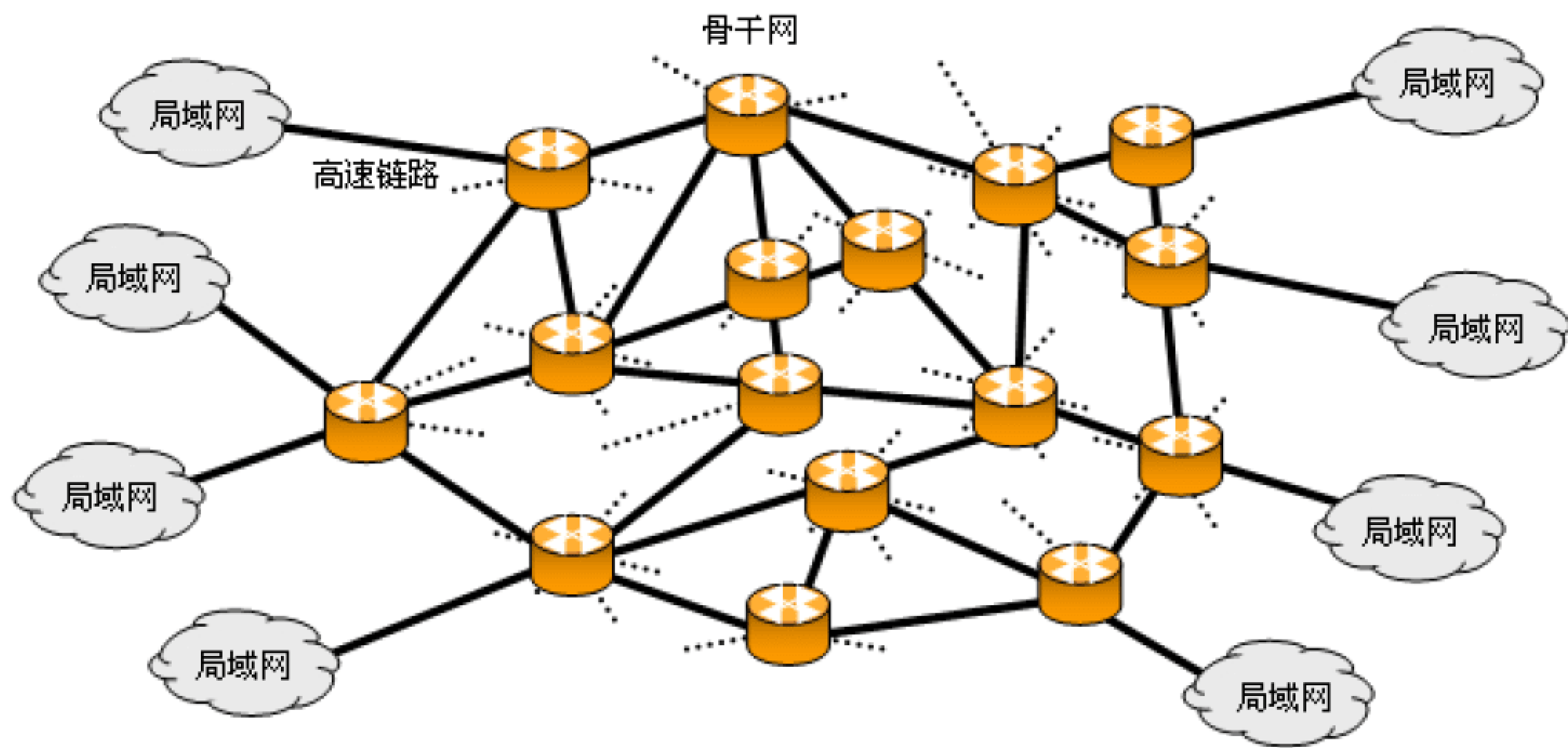


图 1-2　网络互联和高速网络

1.2　网络体系结构

网络体系结构，包含网络协议如何分层、各层协议、层间接口三个方面的内容。

如何分层，是指该协议体系中，共分为几个层次，每个层次的名称、功能分别是什么。例如，OSI 七层参考模型包含物理层、链路层等七个层次，而 TCP/IP 体系结构则分为链路层、网络层、传输层、应用层四个层次。

通过网络进行通信的两个对象都包含着协议体系中的各个层次。两个对象中，处于相同位置的层次，称为对等层。图 1-3 中，用虚线标明了通信中的 A、B 两个对象的对等层示例。对等层内完成通信动作的主体，称为对等层实体，如图 1-3 中的圆形区域。对等层间进行数据交换等通信动作时所遵循的规范，则称为网络体系结构的各层协议。例如，主机 A 的网络层实体发送了一个数据包给主机 B，这个数据包的包结构、包内各字段的定义，都必须遵循网络层协议。

层间接口描述的是某通信对象内不同网络层次间进行数据交换时所遵循的规范，其所处位置见图 1-3 中的方块形区域。

也许有人会问，为什么网络体系结构一定要分层？事实上，基于前人的大量经验，非常确定的是，在设计一个比较复杂的系统时，如果不对系统进行分解，并对分解后的各部分进行独立设计，同时降低各部分间的耦合度，那么在系统后续运行、维护、调整中，系统内大量相互牵扯的因素将导致牵一发而动全身，这些被“动了的全身”进而会引发更多的问题，最终整个系统将变得不可管理、不可维护。

基于上述原因，为了有效运行、管理、维护复杂系统，并提高设计效率，必须将系统进行分解。对复杂系统的分解，通常有分层和分块两种方式。程序设计中的模块化编程、面向对象编程，都是典型的以分块的方式来分解复杂系统的手段，而操作系统的分层设计、网络协议的层次结构，则是分层分解方式的典型。

分层在复杂系统设计中带来的效率、可维护性的提升是不容置疑的，但分层也并非是毫无“副作用”的灵丹妙药。层次的划分，在系统运行过程中需要一定的开销，会造成部分性能损失，随着硬件运行速度的迅猛发展，与设计效率的提高及系统可维护性相比，这种性能损失是完全可以接受乃至忽略不计的。

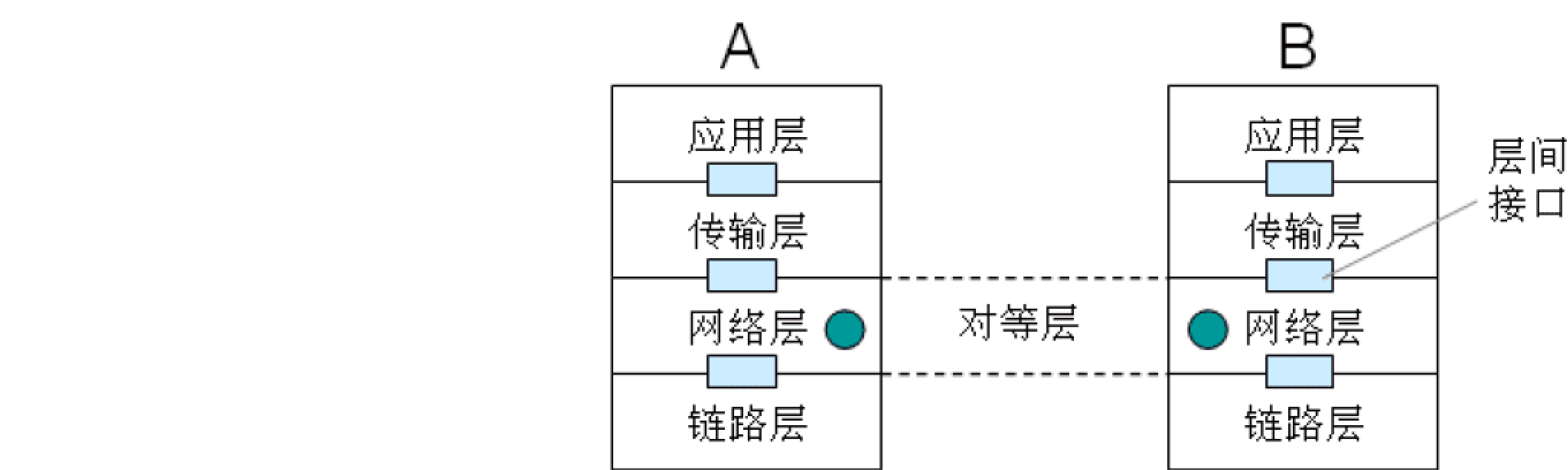


图 1-3　对等层、对等层实体、层间接口

1.2.1　OSI 参考模型

OSI 开放系统互联参考模型把网络分为七个层次，如图 1-4 所示，从下往上，依次称为第一层、第二层，直至第七层。其中物理层、链路层、网络层通常用于在网络中传递数据，构成整个网络的通信子网。而组成资源子网的各类主机，不仅包含第一至第三层协议，还涵盖第三层以上用于保障数据正确传输、实现多种多样网络应用功能的各层协议。

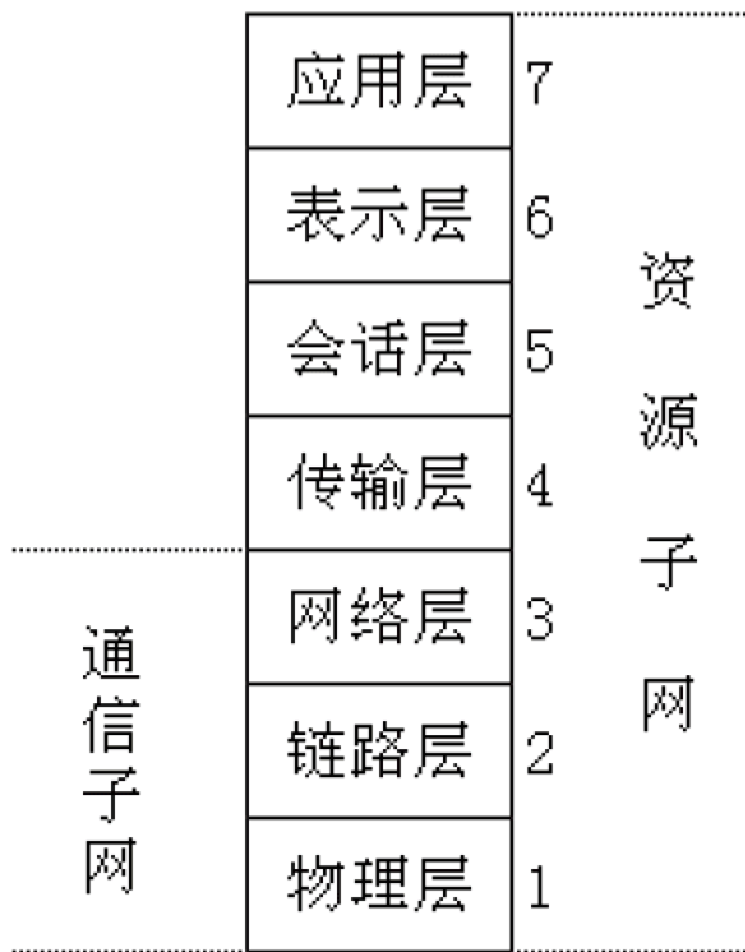


图 1-4　OSI 七层模型示意图

需要注意的是，OSI 与 ISO 常常容易混淆。OSI 是一个具体的规范标准，而 ISO 是制定标准的机构。OSI 是 ISO 制定的标准之一，ISO 还制定了许多其他标准，比如，日程生活中常见的 ISO 9001 标准，就是 ISO 9000 系列所包括的一组质量管理体系的核心标准之一。在许多日用品的包装上可看到 ISO 9001 标志，这通常意味着某种程度上的品质保障。

传输网络数据的光纤、双绞线等物理介质位于物理层之下。而物理层的功能在于，定义网络连接器有多少帧、什么样的信号表示“1”、什么样的信号表示“0”、每个“1”或“0”在信道上持续多长时间等机械、电气规范。

链路层的主要功能是媒体访问控制、帧同步、流量控制。在采用广播信道的网络中，信道被多个主机共享，因而存在对共享信道的访问冲突，媒体访问控制用于管理对共享信道的访问，以减少冲突，并有效处理发生的冲突。帧同步，指的是识别物理传输介质上连续的“0”、“1”比特流，从中分离出一个一个的帧(Frame)，如图 1-5 所示，其中深色部分代表识别出的一个帧。流量控制则用于协调数据发送、接收双方的数据传输率，以实现在数据正确传输的前提下，尽可能提高传输效率。

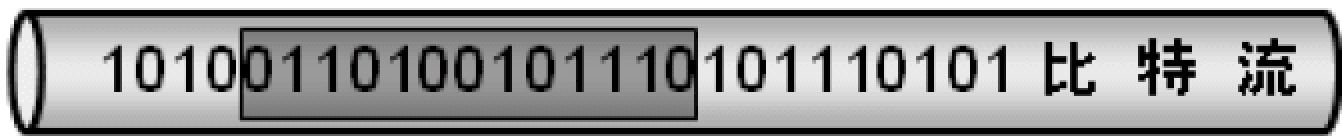


图 1-5　帧同步示意图

简单地说，网络层的功能在于编址和寻址。编址类似于为某个小区的住户分配门牌号码，其作用是为网络中的不同主机分配不同的地址编码，从而加以区分。寻址，网络专业术语称为路由，或称路径选择，是指根据目的主机的地址，来决定数据包应该走向哪条网络路径。

传输层的功能是对网络层功能的进一步扩展，网络层实现将数据传输至目的主机，但数据将会由目的主机中的哪个应用程序来接收处理，则取决于传输层的机制。可以这样理解，网络层提供的是主机端到端的传输能力，而传输层提供的是主机内应用程序端到端的传输能力。

会话层允许不同主机上的用户之间建立会话，包括对话控制、发言管理、同步等服务。

表示层之下的各层，主要关注如何传递数据，而表示层关注的是所传递信息的语法和语义。不同体系结构的计算机可能会使用不同的数据表示方法，为了让这些计算机间能正确通

信，所交换的数据结构必须以一种抽象的方式来定义。一个典型的例子是，在存储数据时，x86 架构的计算机使用的是低位在前(Little-Endian)的方式，比如一个 16 位二进制数 1234H，在内存的低地址字节存放的是 34H，在高地址字节中存放的是 12H，而 PowerPC、SPARC 和 Motorola 处理器则通常使用的是高位在前(Big-Endian)的方式，同样的 1234H，在内存中存放的两个字节的地址顺序则是相反的。

应用层包含了多种根据用户的不同应用需求而制定的协议。

1.2.2　TCP/IP 参考模型

TCP/IP 参考模型分为链路层、网络层、传输层、应用层四个层次。TCP/IP 参考模型和 OSI 七层模型的对应关系如图 1-6 所示。



图 1-6　两种网络体系结构对应关系

显而易见的是，TCP/IP 模型简化了 OSI 模型，这也是 TCP/IP 成为当前网络协议的事实标准的主要原因。事实上，OSI 模型作为国际标准化组织制定的一种网络理论体系结构，从未被真正意义上的产品实现过。

TCP/IP 模型中，对链路层并未作出明确限定，根据网络使用的硬件的不同，支持多种不同的链路层、物理层协议，如以太网、令牌环网、FDDI(Fiber Distributed Data Interface，光纤分布式数据接口)、ATM(Asynchronous Transmission Mode，异步传输模式)及 RS-232 串行线路协议等。因此，为了在针对具体协议进行分析时表述方便，通常将 TCP/IP 模型中的链路层分解为类似 OSI 七层模型的链路层协议、物理层协议。以下针对 TCP/IP 协议网络系统进行分析时，均采用这种方式。

对网络协议进行分析，首先需要了解一次通信过程中数据在各层间流动的情况。在一次数据发送操作中，数据在各层间流动的方向是由上往下，从最高的应用层，向下流向传输层、网络层、链路层、物理层，直至物理线路，如图 1-7 所示。需要强调的是，除了从链路层到物理层，数据在其他各层网络协议间由高层向低层流动时，每下降一层，所传递的数据就会被加上一个相应层次的头部(Header，又称首部)信息。

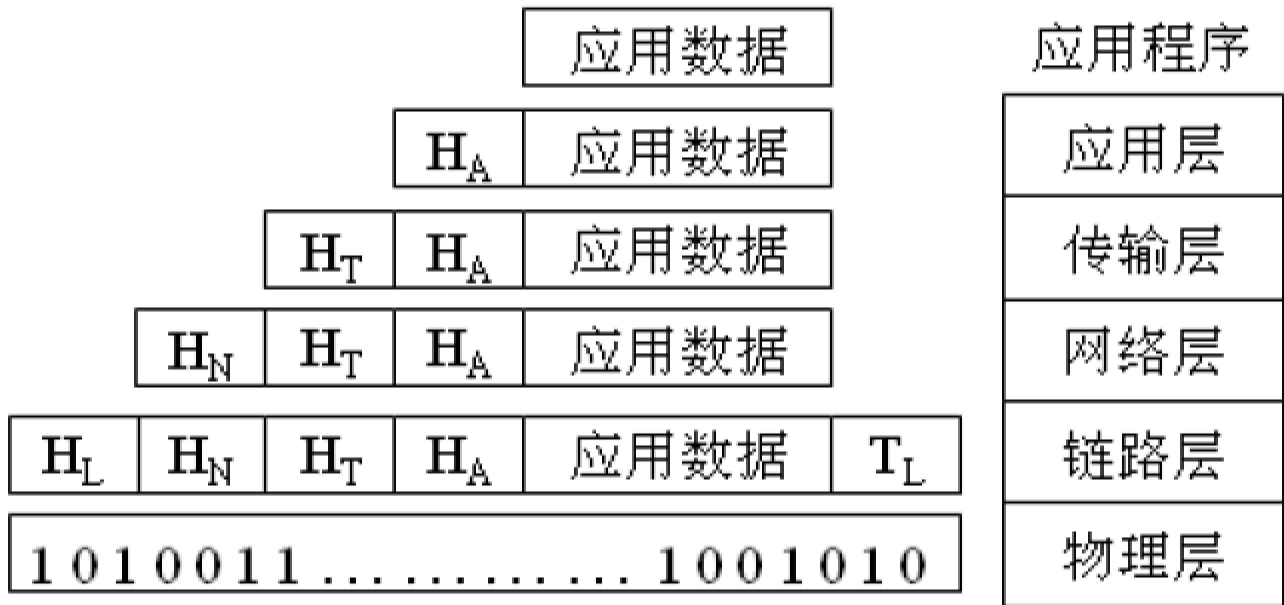


图 1-7　发送过程中，数据在各层间的流动

图 1-7 中，H_A、H_T、H_N、H_L 分别表示应用层头部、传输层头部、网络层头部和链路层头部。数据由高层向低层流动时，除了被加上一个头部信息外，在链路层，还会被加上一个链路层尾部(Tail)，图 1-7 中以 T_L 表示。

下面通过一个实际操作中捕获(Capture)到的网络数据包分析，来验证数据在各层网络协议间的流动过程，如图 1-8 所示。网络数据包的捕获和分析，需要用协议分析工具来完成。网络数据包捕获动作也称为抓包，相关工具的用法将在后文中介绍。

图 1-8 所示是一次 FTP 登录操作中捕获到的网络数据。FTP(File Transfer Protocol，文件传输协议)是被广泛用于在网络上存放、处理文件的协议。

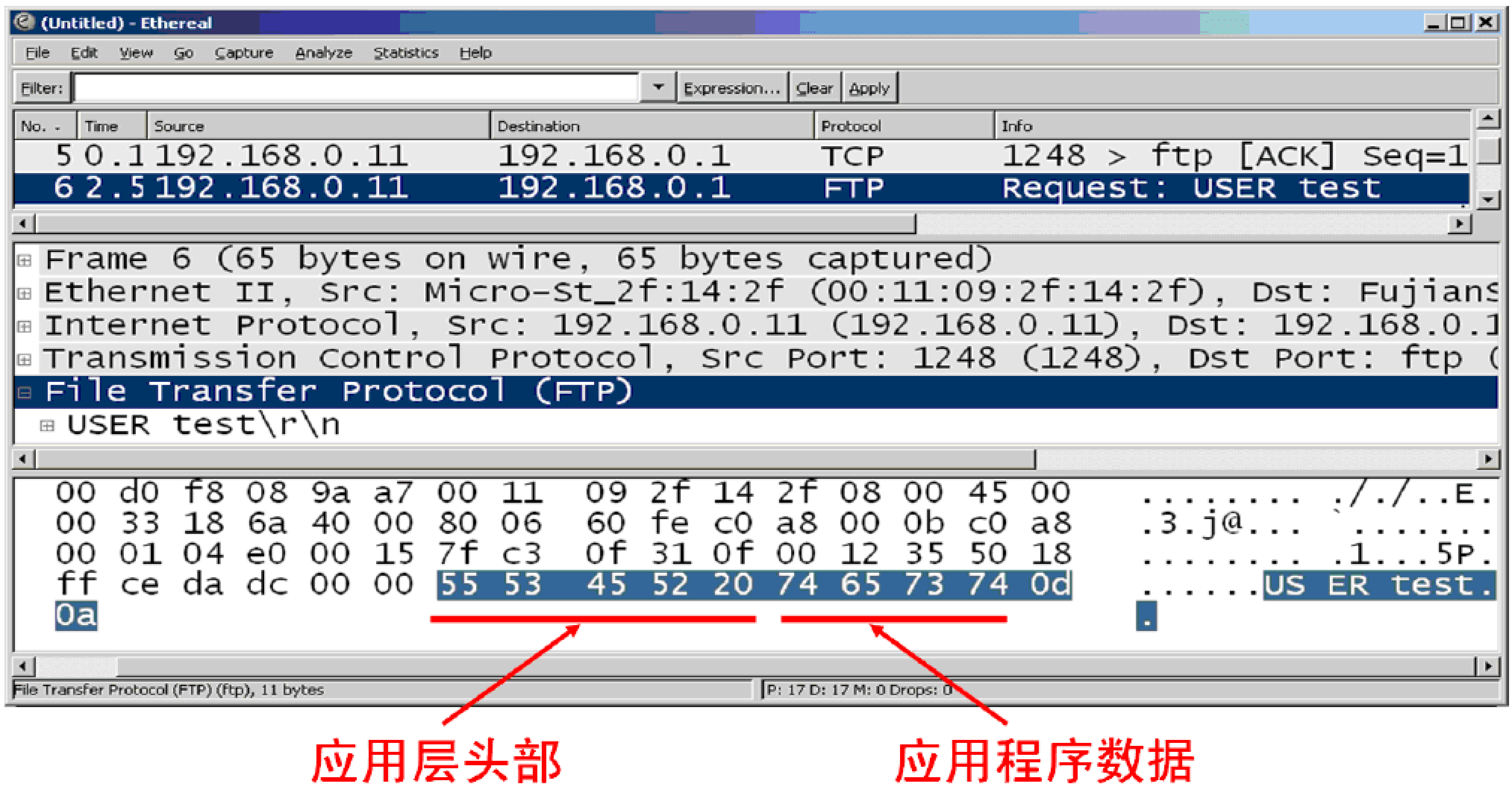


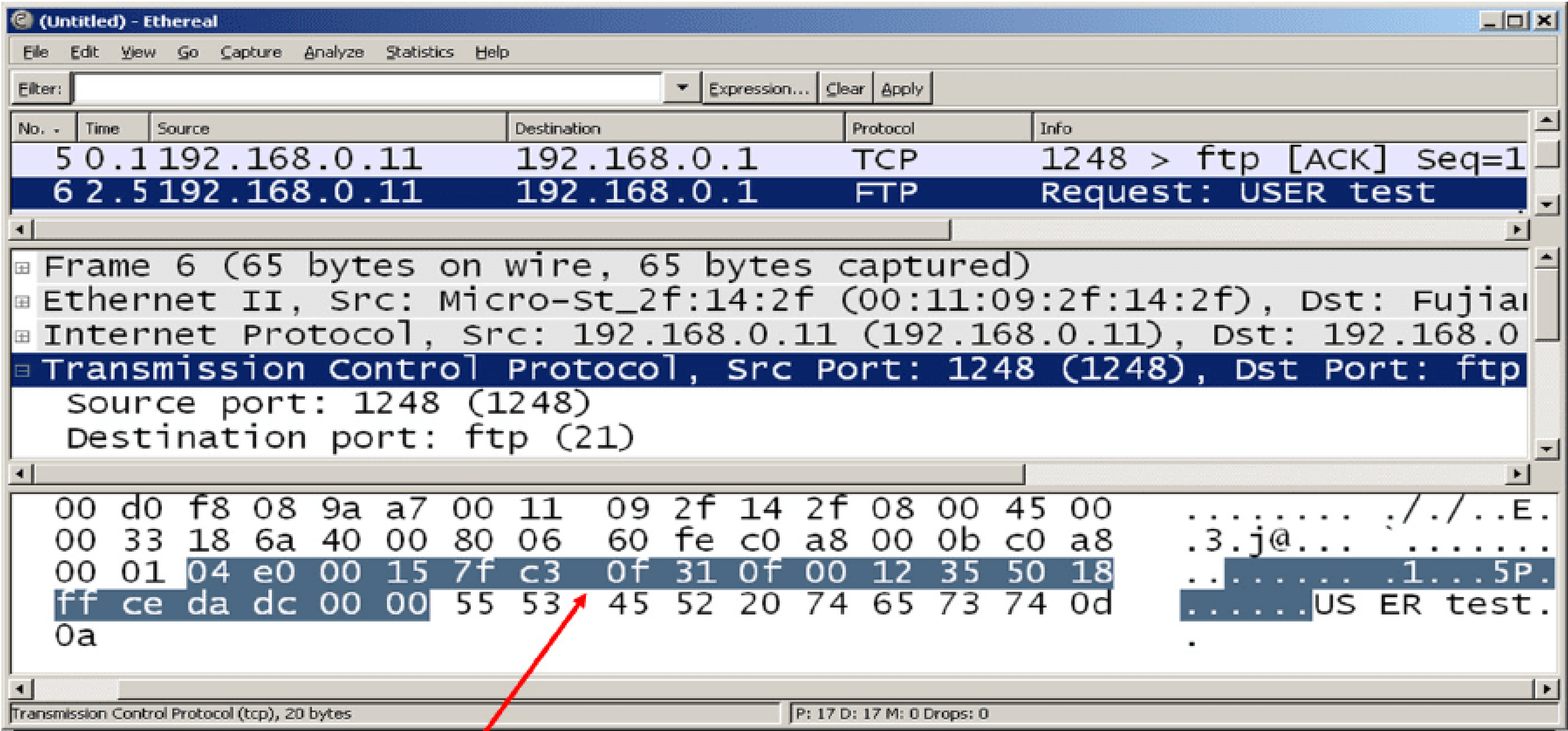
图 1-8　FTP 登录操作过程中的应用层数据

使用 FTP 协议进行网络文件操作，需要输入用户名、口令进行登录。本例中 FTP 客户端的 IP 地址是 192.168.0.11，FTP 服务端的 IP 地址是 192.168.0.1，对应于图 1-8 上方地址信息区域左侧源地址(Source)栏和右侧目的地址(Destination)栏。

图 1-8 中，捕获到的网络数据包被解析为各个层次的协议，见该图中部的协议信息区域。我们从应用层开始对这个数据包进行分析，由图可见，图中部深色部分的“File Transfer Protocol(FTP)”，表明当前的 FTP 操作被准确识别出来了。图下部显示的是当前网络数据包对应的十六进制数据，并在其右侧显示了对应的 ASCII 码。

通过对当前网络数据包十六进制数据及其 ASCII 码的分析，验证了前文所述，应用程序数据在向下流动到应用层时，被加入了应用层头部的概念。本数据包中，应用程序数据是“test”，表明当前要登录 FTP 的用户名是“test”，而当前要做的 FTP 动作是向 FTP 服务器发送用户名，因而被加入的应用层头部信息是“USER”。加入应用层头部信息后，完整的应用层数据在图中数据区以反色方式标记出来。

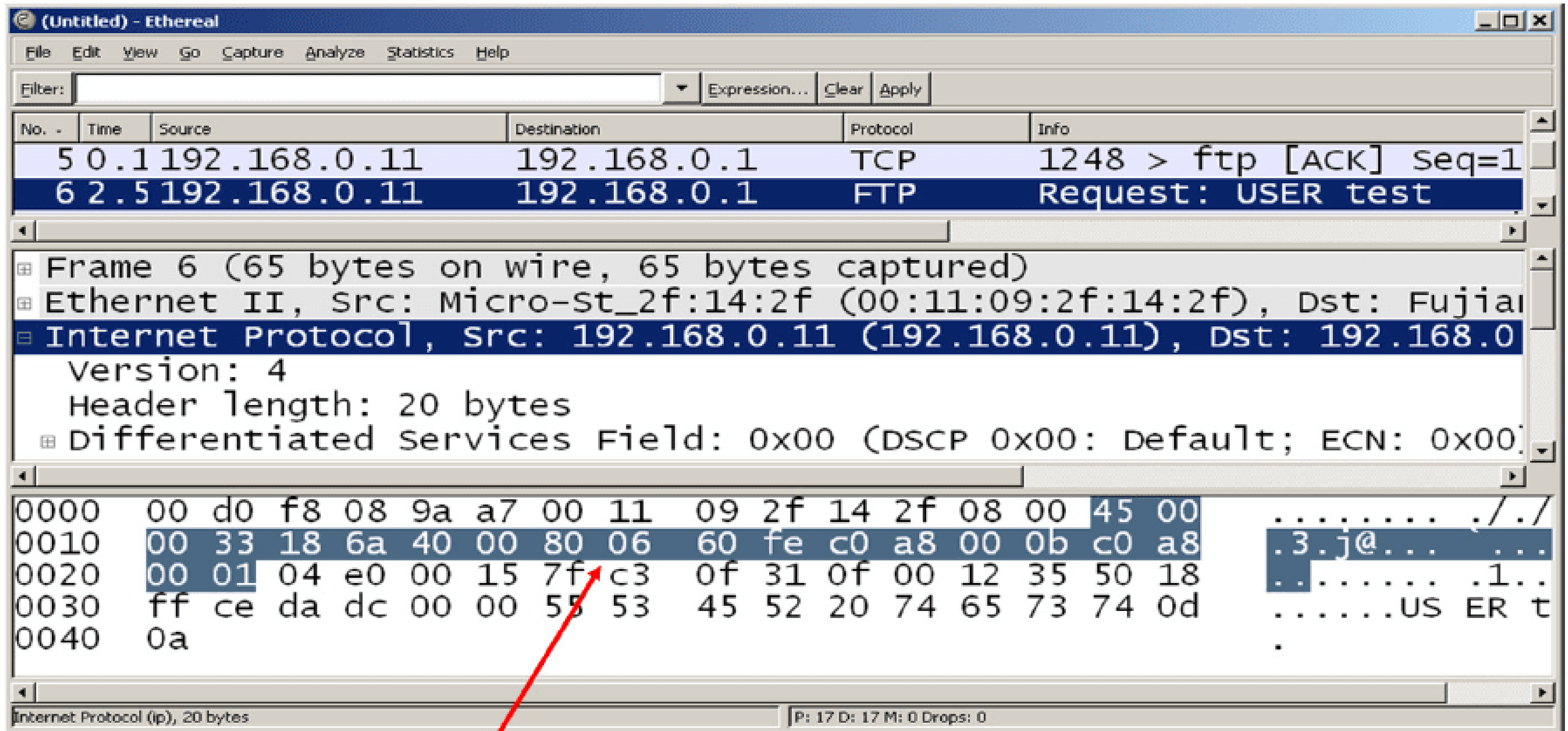
图 1-9 是当前数据包传输层数据的解析。图中部反色部分，表明当前数据包传输层使用的 TCP(Transmission Control Protocol)，其源端口是 1248，目的端口是 FTP(FTP 协议的控制连接使用的默认端口是 21)。通过对图 1-9 中下方数据的观察，结合图 1-8 可以发现，传输层的头部信息，是紧挨着应用层数据的，从而验证了图 1-7 所述，数据向下层流动时，被加入头部信息的概念。



传输层头部

图 1-9　FTP 登录操作过程中的传输层数据

同样的道理，对比图 1-10 和图 1-9 可知，网络层头部也是紧邻着传输层数据。图 1-10 中部解析的数据表明了当前数据包的源 IP、目的 IP 以及使用的 IP 协议版本号。



网络层头部

图 1-10　FTP 登录操作过程中的网络层数据

数据发送过程中，数据由高层流向低层，数据被逐层添加头部信息，到达物理层时，原始应用程序数据已经被加入了应用层头部、传输层头部、网络层头部、链路层头部，并在数据尾部加入了链路层尾部信息，这个过程称为数据封装。

数据到达目的地后，数据流向则变为由低层流向高层，此时，数据每向高层流动一层，则被去掉该层的头部信息，比如，数据由链路层流向网络层，则链路层头部、链路层尾部被去掉，以此类推，直至数据到达接收方的应用程序，这个过程称为解封装。不难理解，到达目的应用程序后，数据已被去掉各层头部信息，还原成原始的应用程序数据。

数据在发送方由高层流向低层直至物理线路，在接收方由低层流向高层直至应用程序，这个过程对各层协议来说，是“透明”的。通过前文对网络体系结构分层的原因分析可知，每层协议只负责完成本层的功能，并与相邻层次交换数据，不关心除此之外的任何其他事情。因此，某协议层次 N 之外其他层次的工作，第 N 层协议完全不知情，也无须了解。例如，发送方的应用程序 1 将数据通过网络传递到接收方的应用程序 2，此过程中实际数据流向是，在发送方向下经历了应用层、传输层、网络层、链路层，到达物理线路，然后在接收方依次向上历经各层，如图 1-11 中的实心箭头方向所指。然而，对数据收发双方的对等层而言，并不了解实际数据的流动过程，而只知道数据从发送方的某层实体发出，在接收方的对等层实

体则可接收到数据。以图 1-11 中传输层的两个对等层实体为例，对接收方的传输层实体而言，它认为数据直接来自于发送方的传输层实体，见图 1-11 中虚线箭头，这就是我们所说的“透明”，两个传输层实体不了解、不关心实际数据的流动方向和流动过程，实际数据的流动过程对两个对等层实体而言是“透明”的。

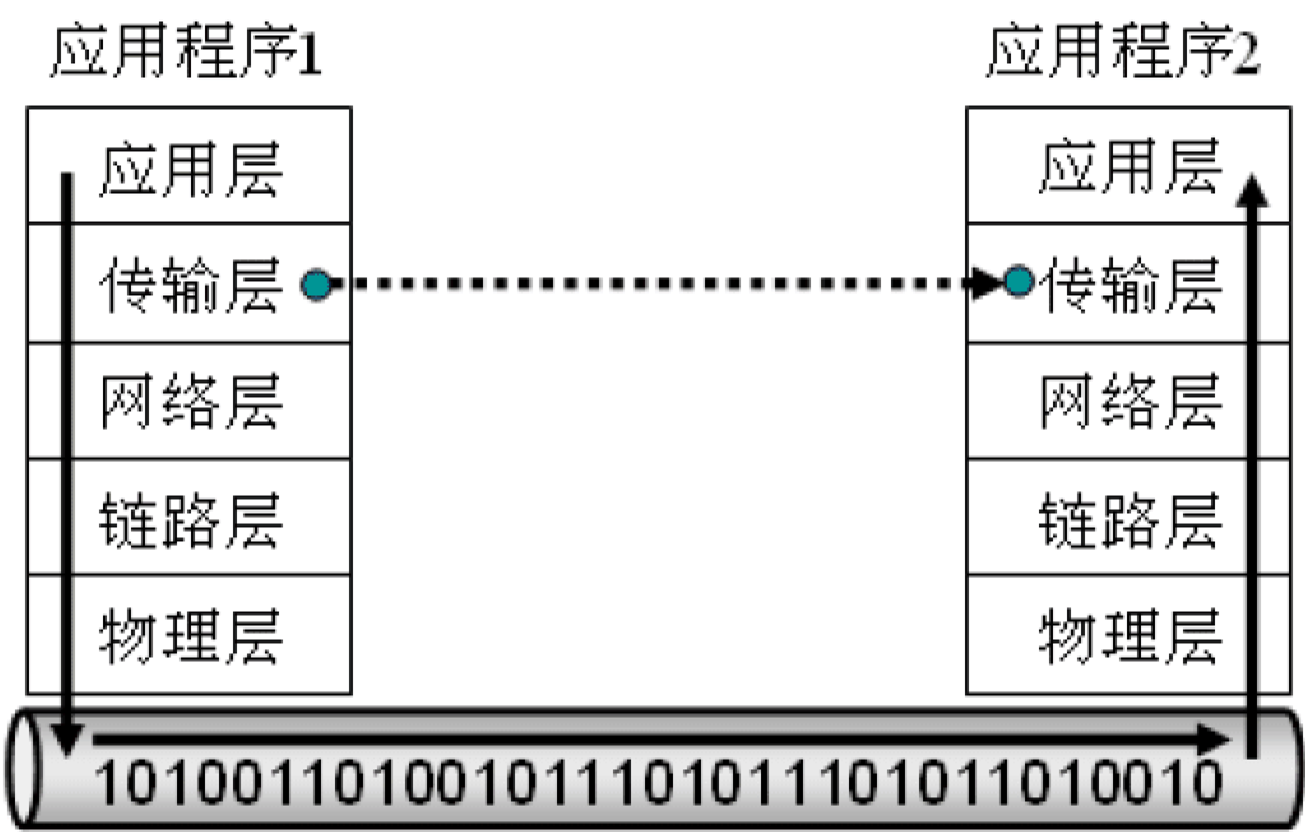


图 1-11　实际数据流向、对等层数据流向

1.3　TCP/IP 协议基础

计算机网络的鼻祖——ARPANET，是由美国国防部资助的一个研究性网络，最初是为军事目的而设计的，其基本思路是，当局部地区因战争等原因遭受打击、破坏时，全国范围的骨干网络能保持正常运行，以保障通信、指挥系统的运转。除此之外，这个网络还需要具备无缝连接多种网络的能力。经过一段时间的发展，ARPANET 所采用的网络体系结构逐渐演变为 TCP/IP 参考模型。全球范围的 Internet，正是基于 ARPANET 发展壮大的，因此，TCP/IP 参考模型被称为事实上的网络标准。

1.3.1　链路层协议

为了实现多种不同类型网络的互联，TCP/IP 协议体系的链路层并没有定义具体内容，而是采取直接支持以太网、令牌环网、FDDI、ATM 异步传输模式)及 RS-232 等多种链路层、物理层协议的方式。也就是说，这些成熟的链路层协议，可直接应用于 TCP/IP 体系。

在 TCP/IP 所支持的链路层协议中，令牌环网已是昨日黄花，而以太网经过三十余年的发展，因为其简单易用、技术规范标准化、更新快、厂家支持等原因，正处于如日中天的阶段。目前，发展初期定位为局域网的以太网，有日益向广域网延伸的趋势。

日常生活中，经常看到、听到的“以太网”这个名词，究竟是什么意思？这个概念有着什么样的内涵？这是我们需要明确的问题。

首先要了解的是，以太网是局域网的一种。局域网，是连接小范围地理区域的通信网络。局域网通常使用广播信道/多路访问信道，主要关注的是对共享信道的访问控制，我们知道，这正是链路层协议的主要内容。广播信道，意味着网络上的所有节点共享同一信道，一个节点发出数据，所有其他节点都能收到此数据。当多个节点同时发送数据时，则会导致信道冲

突(Collision)，因此需要信道访问控制。除以太网以外，典型的局域网类型有令牌环网(目前已被淘汰)、FDDI 网络、ATM 网络等。

局域网规范由链路层协议和物理层协议构成，作为目前最为广泛应用的局域网，以太网由一系列协议标准构成。1979 年初，美国施乐(Xerox)公司和 DEC 公司共同提出建造以太网的设想，其后，Intel 的加入加速了以太网的发展。1980 年 9 月 30 日，DEC、Intel 和施乐公布了“以太网，一种局域网：数据链路层和物理层规范，1.0 版”，即著名的以太网蓝皮书，也称为 DIX 以太网 1.0 规范。1982 年公布了 DIX 以太网 2.0 规范。IEEE 成立了一个定义与促进工业局域网标准的名为“802 工程”的委员会，1981 年 6 月，IEEE 成立了 802.3 分委员会，负责基于 DIX 2.0 规范的标准化。IEEE 802.3 涵盖了物理层协议、链路层的媒体访问控制协议。因此，在不严格区分时，以太网、DIX 2.0、IEEE 802.3 三者通常被看做同一事物。IEEE 802.3 的媒体访问控制协议是 CSMA/CD(Carrier Sense Multiple Access with Collision Detection，带冲突检测的载波监听多路访问)，这也是以太网的基本标志。

由此可以这样描述，以太网是采用 CSMA/CD 媒体访问控制协议的一种局域网类型，由一系列 IEEE 802 协议规范。典型的其他局域网还有令牌环网、FDDI 网、ATM 网。

以太网所采用的 CSMA/CD，意味着按照如下方式来访问共享的信道。Multiple Access，即多路访问，表明多台主机连接到同一总线上，即多主机共享信道，不能同时发送数据。Carrier Sense，载波监听，意指在主机发送数据前，需要先检测总线上是否有其他主机正在发送，如有，则暂时不发送，以免发生冲突。载波监听机制并不能完全避免冲突产生，考虑如图 1-12 的情况，在 t_0 时刻，信道空闲，主机 A 开始发送数据，在经历了一定时间后的 t_1 时刻，另一主机 B 要发送数据，基于载波监听的机制，B 首先检测总线是否空闲，由于信号在物理线路上传递需要时间，A 发出的数据尚未到达 B，因而此时 B 会误以为总线处于空闲状态，也开始发送数据，则 A 发出的数据和 B 发出的数据会在 t_2 时刻相遇，从而产生冲突。产生冲突后，总线上的数据处于不确定状态，A 和 B 都需要重新发送，冲突检测(Collision Detection)机制就是为此设置的。为了避免 A 和 B 重新发送数据时又产生冲突，通常采取的方法是，令 A 和 B 都等待一个随机时间段，然后再次进行载波监听，并在总线空闲的条件下重发数据。冲突检测是伴随着数据发送动作一直进行的，即一边发送数据，一边检测冲突，一旦出现冲突，马上停止数据发送。

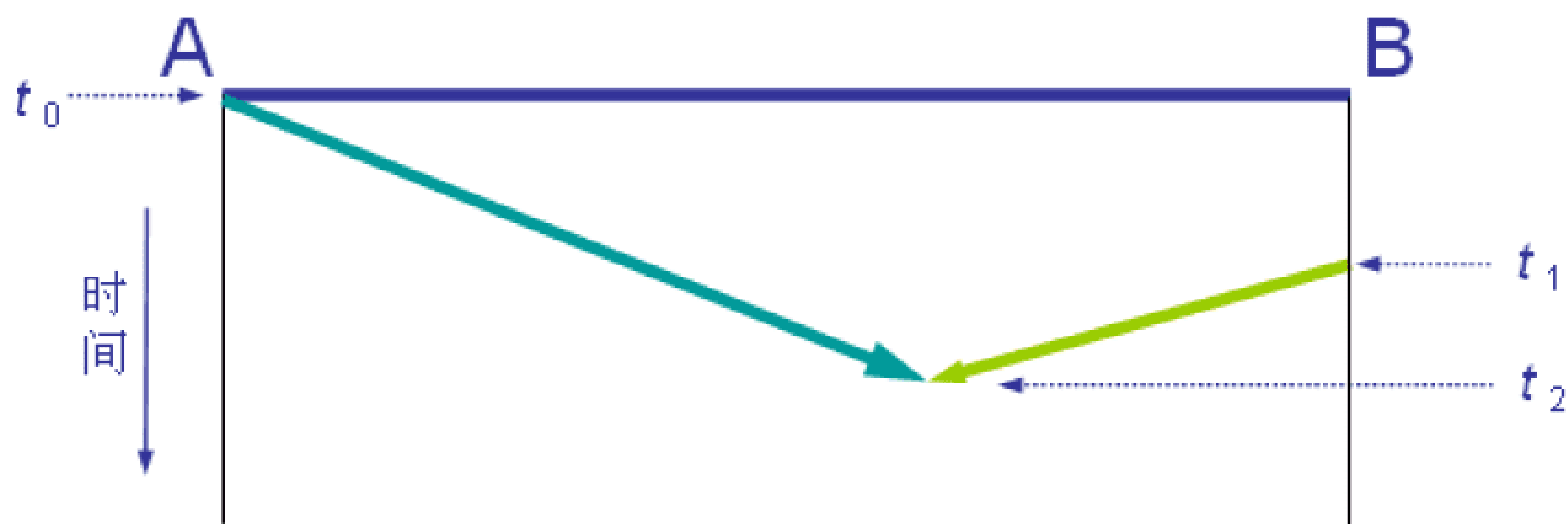


图 1-12　载波监听情况下，可能发生冲突

根据 CSMA/CD 的工作原理可知，这种媒体访问控制协议，工作原理比较简单，实现相对容易，在总线不繁忙的情况下，产生冲突的概率较低，网络通信系统能有效运转。然而，当总线上的通信数据量比较大时，产生冲突的概率则大幅上升，冲突越多，意味着各主机的

链路层就要进入随机等待状态，而不能传输数据，当总线负载很重时，几乎所有的时间都用在冲突处理上，整个信道的利用率变得极低甚至接近于零。

另一种典型的媒体访问控制协议是令牌环网所采用的协议，称为令牌环协议，如图 1-13 所示。令牌环网的线路由一个环形总线组成。总线空闲时，有一个令牌绕环运行，所有主机只有获得令牌后才能发送数据。获得令牌的主机，在发送数据前，先删除令牌，发出一份数据后，该主机则产生一个新的令牌。令牌环协议的工作原理决定了在这种网络中，不会产生冲突，网络上的所有主机享有均等的发送数据的机会。在通信负载很重的情况下，信道利用率接近 100%。然而，令牌环网的环形总线结构，在网络连接方式、所需硬件支持上，都比较复杂、成本较高。其技术标准不够开放，与以太网相比更新明显滞后，目前这种局域网类型已被淘汰。

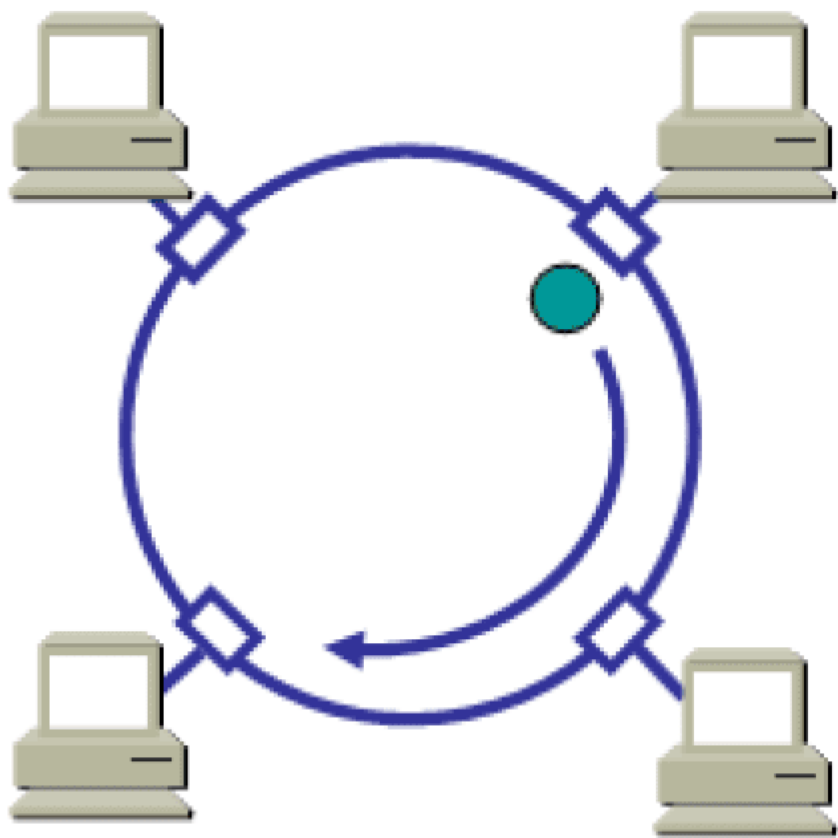


图 1-13　令牌环网的媒体访问控制

两台主机的链路层实体间通信时，为了识别不同主机，所使用的地址称为物理地址，物理地址是附着在主机的网络接口卡(俗称网卡)或网络适配器上的，故物理地址又称硬件地址。由于以太网在局域网领域的绝对统治地位，在不严格加以区分的时候，以太网所使用的媒体访问控制(Media Access Control，MAC)地址也被称为物理地址或硬件地址。严格来讲，MAC 地址只是物理地址(硬件地址)的一种。

安装了 Windows 系统的主机，可以按如下操作来查看当前网卡的 MAC 地址。首先单击“开始”菜单，在其中选择“运行”菜单项，在弹出的对话框中输入“cmd”，然后按 Enter 键，进入命令行模式。在命令行模式中输入“ipconfig /all”命令，则可查看当前网卡的相应信息，如图 1-14 中的深色部分。在 UNIX/Linux 系统主机中，则可使用 ifconfig 命令来查看网卡的 MAC 地址。

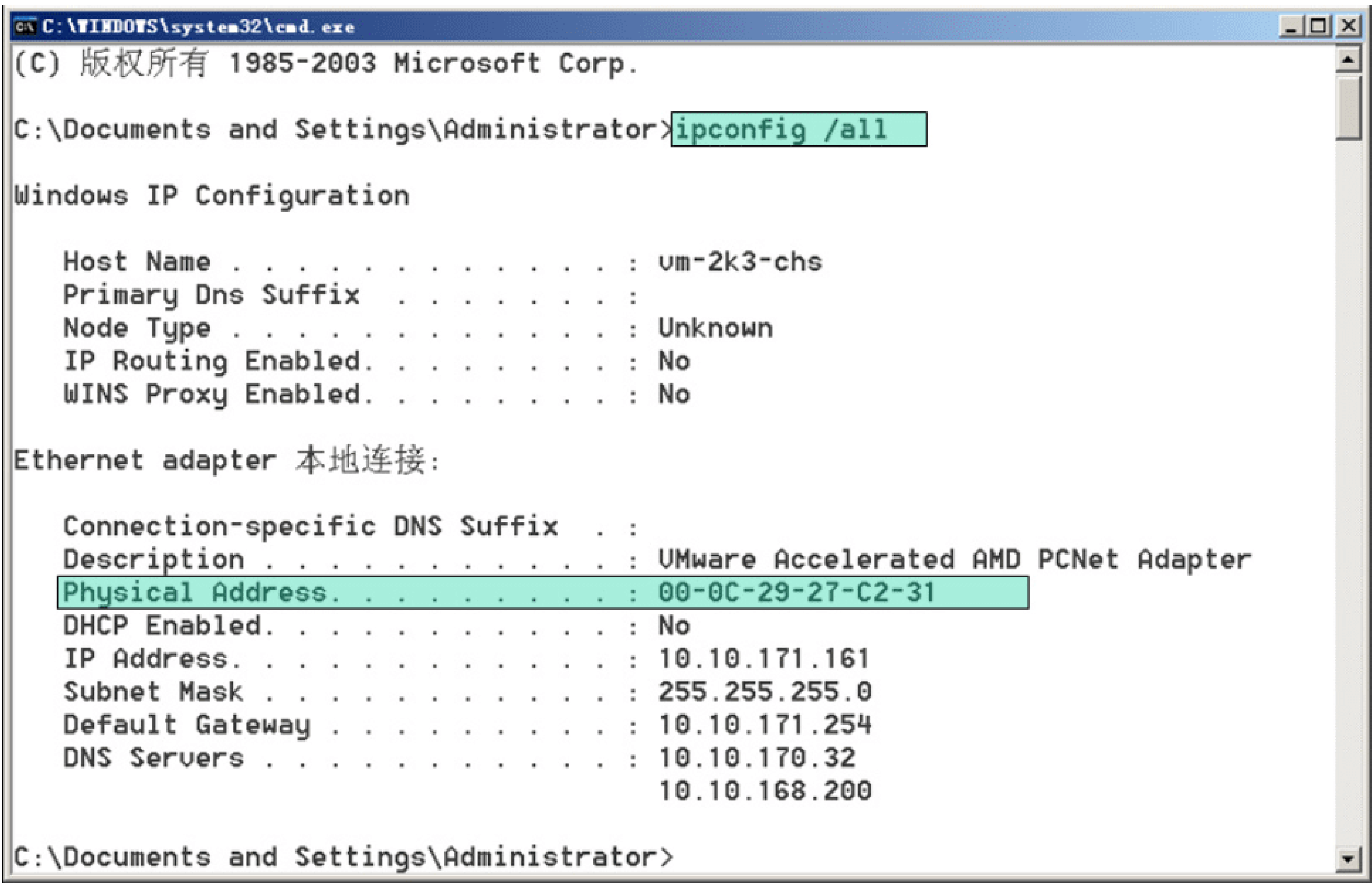


图 1-14　查看网卡的 MAC 地址

由图 1-14 可知，MAC 地址由 6 个字节(48 比特)组成。合法的 MAC 地址在全球都是唯一的，其中前 3 个字节是生产网卡的厂家的代码，后 3 个字节是序号。若某个 MAC 地址的 48 个比特全部为“1”，即 FF-FF-FF-FF-FF-FF，则代表广播地址，向广播地址发送的数据，局域网内的所有主机都能收到并处理。当网卡收到的数据内的地址不是广播地址，也不是本网卡的 MAC 地址时，则会直接将其丢弃。

链路层发送、接收的数据单位，称为帧。以太网的帧结构如图 1-15 所示，长度单位是字节。图中的目的地址、源地址、类型字段，即为链路层的头部信息；校验字段，即为链路层的尾部信息；数据字段，是链路层所运载的高层协议的数据，称为链路层的有效载荷(Payload)。传统以太网(DIX 2.0)帧的有效载荷长度范围是 46~1500 字节。

	目的地址	源地址	类型	数 据	校验
长度	6	6	2	46 ~ 1500	4

图 1-15　以太网的帧结构

由图 1-15 可见，以太网的帧头长度为 6＋6＋2＝14 字节，帧尾 4 个字节，帧头帧尾合计占用 18 个字节，由此可知，传统以太网最短的帧长度为 18＋46＝64 字节，最大的帧长度为 18＋1500＝1518 字节。

以太网帧中的“类型”字段，用于描述帧的有效载荷的协议数据类型。例如，若链路层的上一层协议——网络层使用的是 IP 协议，则类型字段的值为 800H。

1.3.2　网络层协议

作为网络层的主要功能，编址和寻址的功能在 TCP/IP 体系中都是以 IP 地址来体现的。链路层的物理地址，只能实现单一局域网内不同主机的区分与定位，要实现跨局域网乃至整个 Internet 范围的主机定位，则必须使用网络层的 IP 地址。本书中都以当前常用的 IPv4，即 IP 地址的版本 4 为例。

图 1-14 所示的 ipconfig 命令，同样可以用于查看当前主机的 IP 地址，该例中附着于网卡上的 IP 地址在“IP Address”一栏中被列出。IP 地址是一个 32 比特的数字，通常按每 8 位一个字节的方式，用 4 个十进制数以“.”号隔开，称为 IP 地址“点分十进制”表示法。例如，许多家庭上网所使用的宽带路由器，默认的 IP 地址通常是“192.168.1.1”。

IP 地址在整个网络中都是唯一的。需要注意的是，一个网卡上可以设置多个 IP 地址，但一个地址不能同时设置在多个网卡上。IP 地址类似于门牌号码，若两栋房子具有同样的门牌号码，显然会令找路的人陷入困惑。

IP 地址通常可以被理解为网络号、主机号两级层次结构。网络号类似于我们拨打长途电话时的区号，而主机号可看作是区内号码。按网络号、主机号的长度不同，普通用于主机的 IP 地址可分为 A、B、C 三类，如图 1-16 所示。

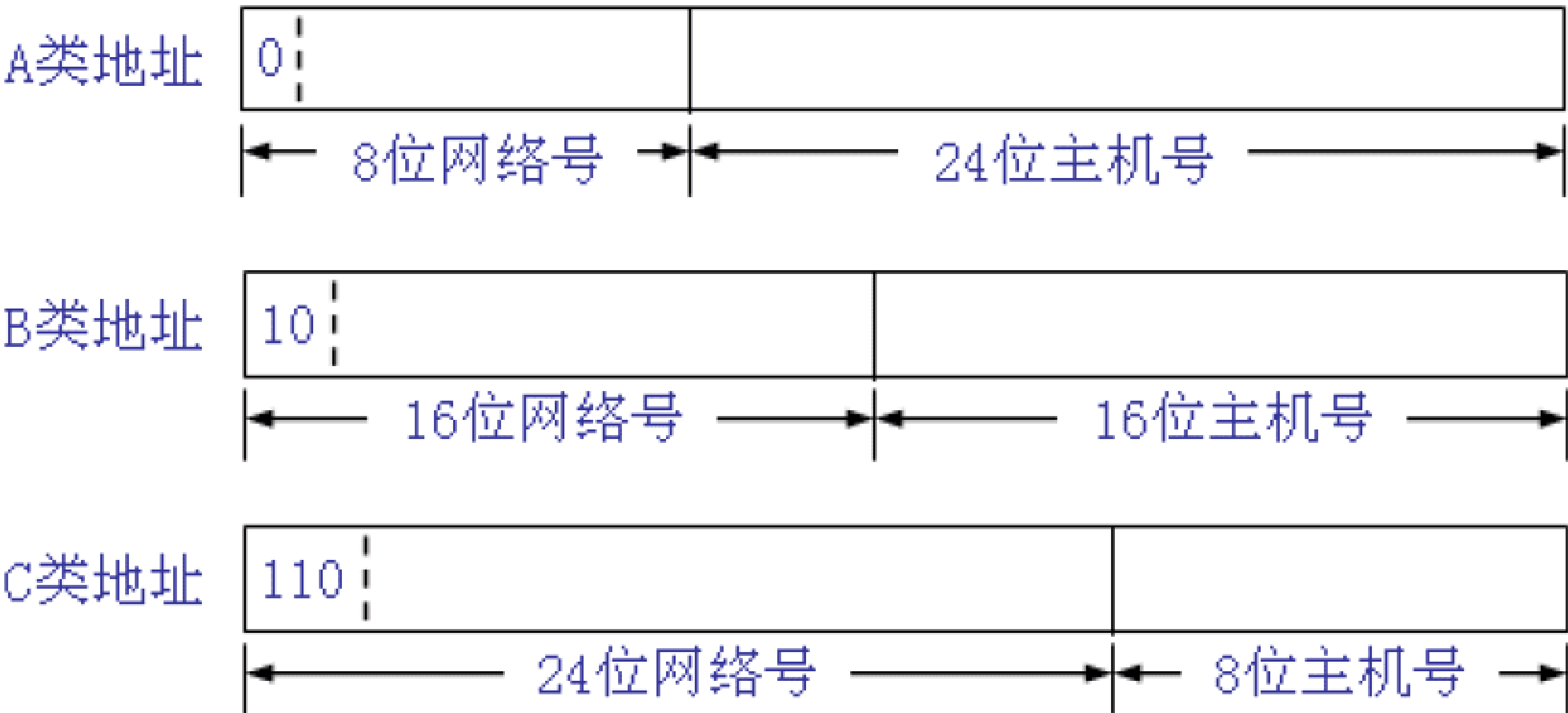


图 1-16　三类 IP 地址

A 类 IP 地址的网络号部分最高位固定为 0，故网络号部分最小值为 0，最大值为 01111111B(B 代表二进制数，此数对应十进制的 127)，其中 0 保留不用，127 用于表示主机自身的环回(Loopback)地址，环回地址用于在没有网络环境的主机上测试网络应用程序。因去掉了 0 和 127，故 A 类地址的可用网络号范围为 0～126。

A 类地址的主机号部分若为全 0，则该 IP 代表一个网络，若为全 1，则该 IP 代表此网络的广播地址。A 类地址具有 24 位主机号，去掉全 0 和全 1 的两个 IP，则可用于主机的 IP 地址有 $2^{24}-2$ 个。

以 IP 位 61.187.54.10 的 A 类地址为例，列出其十进制、二进制对照如下。

61　　　　　. 187　　　　. 54　　　　. 10

00111101　　. 10111011　　. 00110110　　. 00001010

若后 24 比特全部为 0，即成为 61.0.0.0，这就是 61.187.54.10 所在网络的网络地址。

若后 24 比特全部为 1，成为 61.255.255.255，即 61.187.54.10 所在网络的广播地址。

本例中，61.187.54.10 所在网络的可用主机 IP 地址范围是 61.0.0.1 到 61.255.255.254，总共有 $2^{24}-2$ 个 IP 地址。

用类似的方法，可快速计算出 B 类、C 类 IP 地址的网络号范围、网络数、主机号范围、主机地址空间、可容纳的主机数，如表 1-1 所示。

表 1-1　三类 IP 地址空间

IP 地址	网络号范围	网　络　数	主机号范围	主机地址空间	可容纳的主机数
A 类	1~126	2^7-2=126	0.01~255.255.254	1.0.0.1~126.255.255.254	$2^{24}-2$=16777214
B 类	128.0~191.255	2^{14}=16384	0.1~255.254	128.0.0.1~192.255.255..254	$2^{16}-2$=65534
C 类	192.0.0~223.255.255	2^{21}=2097152	1~254	192.0.0.1~223.255.255.254	2^8-2=254

由表 1-1 可知，A 类 IP 地址空间可容纳 10 000 000 个 IP，B 类 IP 地址空间可容纳 60 000 多个 IP，而 C 类 IP 地址空间仅能容纳 200 多个 IP，对 IP 地址分配的粒度差异太大。为了实现 IP 地址的灵活分配，实际采用的方式打破了传统 A、B、C 三类地址的固定长度网络号的模式，而是将大的网络分解为多个小的网络，即划分子网(Subnetting)，或将多个小的网络合并为规模适中的中型网络，即构造超网(Supernetting)。为了叙述方便，通常不严格区分划分子网和构造超网两个概念，而都统称为子网划分。

引入子网划分的概念后，IP 地址的网络号不再只能是 8 位、16 位或 24 位，而是根据实际需要灵活设置。为了描述子网划分中网络号的长度，需要引入子网掩码(Subnet Mask)的概念。和 IP 地址类似，子网掩码是一个 32 比特的数字，它与 IP 地址中的 32 位一一对应，若 IP 地址中的某一位为网络号，则子网掩码对应位为 1，否则为 0。因 IP 地址的网络号必然是在高位，主机号在低位，且网络号部分和主机号部分不会夹杂出现，因而子网掩码必须是 1 在高位(左侧)，0 在低位(右侧)，形如 11..11 00..000。

下面是一个说明子网掩码概念的例子。

【例 1】 已知 IP：128.1.1.6，子网掩码：255.255.128.0，求该 IP 所在子网的网络地址、广播地址、可用主机 IP 地址范围。

首先列出该 IP、子网掩码的十进制、二进制形式如下：

IP 地址	128	. 1	. 1	. 6
即	10000000	. 00000001	. 00000001	. 00000110
子网掩码	11111111	. 11111111	.10000000	. 00000000

将主机号部分全部改为 0，即为网络地址：

网络地址	10000000	. 00000001	. 00000000	. 00000000
即	128	. 1	. 0	. 0

将主机号部分全部改为 1，即为广播地址：

广播地址	10000000	. 00000001	. 01111111	. 11111111
即	128	. 1	. 127	. 255

可得该 IP 所在网络的网络地址为 128.1.0.0，广播地址为 128.1.127.255，可用主机 IP 地址范围是 128.1.0.1~128.1.127.254。

子网掩码也可以用单个数字表示，这个数字来自于子网掩码中二进制 1 的个数。例如，上面的例子中，子网掩码为 255.255.128.0，其中包含了 17 个二进制 1，则我们称此子网掩码长度为 17，该 IP 地址可表示为 128.1.1.6/17。

下面是一个运用子网掩码的概念实现子网划分的例子。

【例 2】 某公司有 A、B、C 三个部门，部门 A 有 180 台 PC，部门 B 有 1200 台 PC，部门 C 有 120 台 PC，各部门的 PC 要求划分到不同子网中。如何从一个 B 类网络 166.111.0.0/16 的低地址段分出大小最合适的三个子网？(要求写出各子网可用主机的 IP 范围)。

进行子网划分，首先要明确划分时的基本原则。

子网太大(主机号太长)，浪费可用主机 IP 地址空间。子网太小(主机号太短)，主机 IP 地址空间不够用。

因此需要以 2^n 为单位，寻找最接近(且大于等于)所需主机 IP 数量的 2^n。

先来看部门 A。部门 A 所需主机数为 180；$2^7=128$，$2^8=256$；最接近(且大于等于)180 的数为 256，故需要 8 位来表示主机号，又 32－8＝24，故为部门 A 划分子网：166.111.0.0/24，子网掩码：255.255.255.0，因此可用主机 IP：166.111.0.1~166.111.0.254。

再来看部门 B。部门 B 所需主机数为 1200；$2^{10}=1024$，$2^{11}=2048$；最接近(且大于等于)1200 的数为 2048，故需要 11 位来表示主机号，又 32－11＝21，故为部门 B 划分子网：166.111.1.0/21，

子网掩码：255.255.248.0，因此可用主机 IP：166.111.1.1~166.111.8.254。

表面上看，对部门 B 的 IP 地址划分已经完成，但我们用类似例 1 的方法，对 166.111.1.0/21 这个地址空间进行运算，就可以发现，这个地址空间所覆盖的 IP 地址范围是 166.111.0.0~166.111.7.255。这会导致什么问题呢？对比前面已经划分给部门 A 的地址空间，可以发现，当前给部门 B 划分的空间覆盖了部门 A 的空间。因此当前的划分方法是错误的。

导致这个错误的原因在于，对 IP 地址进行划分时，是以 2^{32-n} 为单位进行的，其中 n 为子网掩码长度。例如子网掩码长度为 21，则划分出的 IP 地址空间将以 2^{11}，即 2048 个 IP 为单位。因此如果要保持划分给部门 A 的 IP 地址空间不变，则必须将部门 B 的 IP 地址空间向后移 2^{11} 个 IP，即紧邻 166.111.1.0/21 的下一个包含 2^{11} 个 IP 的地址段。因 166.111.1.0/21 的地址段为 166.111.0.0~166.111.7.255，故下一个地址段为 166.111.8.0~166.111.15.255，用 IP/子网掩码的方式可表示为 166.111.8.0/21。

最后来看部门 C 的地址划分。

部门 C 所需主机数为 120，2^6=64，2^7=128；最接近(且大于等于)120 的数为 128，故需要 7 位来表示主机号，又 32－7=25，故为部门 C 划分子网：166.111.1.0/25，子网掩码：255.255.255.128，因此可用主机 IP：166.111.1.1~166.111.1.126。

部门 A、B、C 的 IP 地址空间可形象地表示为图 1-17。图中下方是低地址段，上方是高地址段。每一行表示一个 C 类地址段(24 位掩码)。

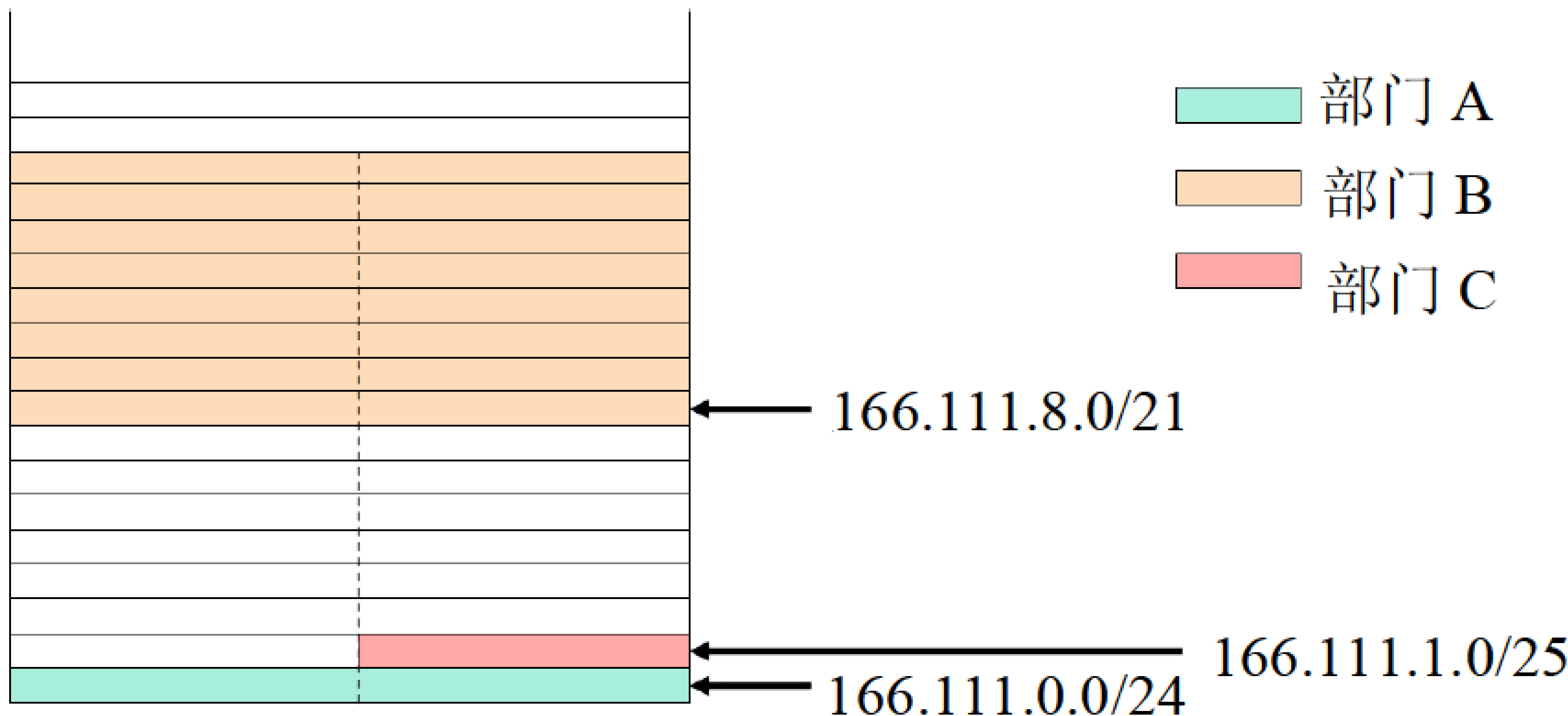


图 1-17　部门 A、B、C 的地址空间

我们已经知道，在数据的发送方，网络层的 IP 数据包(IP Packet)将被封装在链路层的帧里，然后经过物理层发送到网络线路上。在此过程中，对发送方的网络层而言，只知道目的地的 IP 地址，但数据最终要向下流到链路层，通过链路层的某种局域网协议，发送出去。而链路层协议并不能理解封装在帧的有效载荷里面的 IP 地址，链路层只能理解物理地址。因此需要一种机制，在数据由网络层向下流向链路层时，根据目的地的 IP 地址，得到目的地的物理地址(我们以 MAC 地址为主)，这正是处于网络层的 ARP(Address Resolution Protocol，地址解析协议)的功能所在。

对 ARP 协议的理解，有助于分析网络运行状况，判断各种网络故障。例如，某内网主机要访问外网的站点，则它首先必须与自己的网关建立联系，将访问请求发送给网关。而网关必然是与该内网主机在同一网络(局域网)中，否则无法直接联系。因此，通过查看内网主机的 ARP 缓存，检查有没有网关 IP 对应的 ARP 表项，是判断该主机能否访问外网的基本方

法。在 Windows/UNIX/Linux 操作系统中，查看 ARP 表项的命令是一致的，即 arp –a 命令，该命令使用实例如图 1-18 所示。

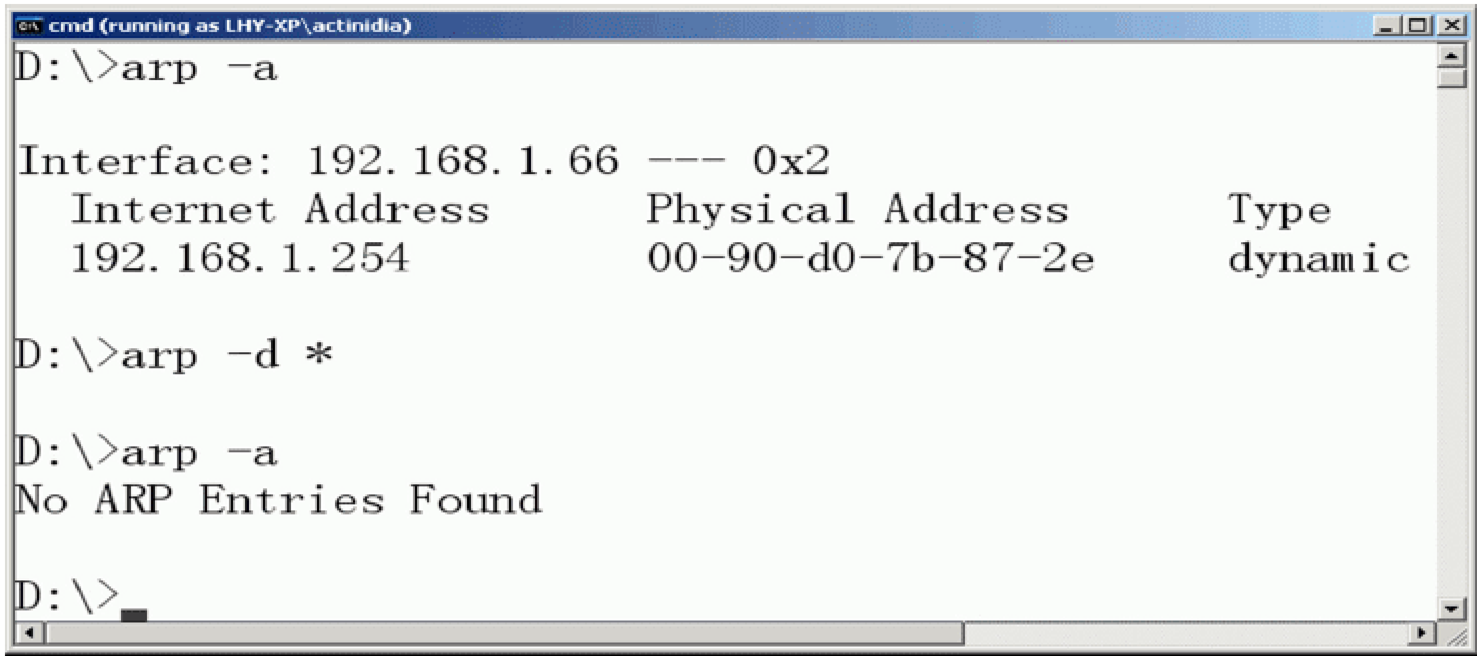


图 1-18　ARP 缓存相关操作

由图 1-18 可见，每一条 ARP 表项由 IP 地址和 MAC 地址相对应。主机与网关正常通信的基本条件就是在 ARP 表项里包含网关 IP 对应的 MAC 地址。arp –a 用于查看 ARP 缓存，arp –d 用于删除 ARP 表项，arp –s 10.10.0.1 00-aa-00-62-c6-09 用于设置静态 ARP 表项。

掌握了 ARP 协议工作的基本原理，以及 IP 地址、MAC 地址间的关系，就可以用简单的 ping 命令来了解主机所在局域网内其他主机的一些情况。例如，主机 A 想了解主机 B 的 MAC 地址，只需在命令行方式下 ping B 的 IP，即使 B 安装了一般的防火墙，它的 TCP/IP 协议栈也会作出响应，将 B 的 MAC 地址返回给主机 A。此时，在主机 A 上按图 1-18 操作，即可发现主机 B 的 ARP 表项。

由于 ARP 协议的工作原理比较简单，缺乏基本的安全机制，利用 ARP 协议进行网络攻击的行为非常普遍，给广大用户的正常网络通信造成严重影响，对用户的数据安全也带来了极大威胁。

利用 ARP 协议进行攻击的典型思路是，向目标主机发出 ARP 响应数据包，里面包含网关的 IP 和错误的 MAC 地址，目标主机收到 ARP 响应数据包后，不会检查数据包的合法性，直接更新其 ARP 缓存，这个过程称为 ARP 欺骗(ARP Spoofing)。遭受 ARP 欺骗的目标主机与网关通信时，会将数据发送到错误的 MAC 地址上，因而与正确的网关失去联系，从而造成与外部网络中断。利用类似的原理，同时使用 ARP 欺骗攻击目标主机和网关，则能实现中间人攻击(Man-in-the-Middle Attack)，从而达到捕获目标主机所有网络通信数据的目的。

图 1-19 演示了利用 ARP 欺骗实现中间人攻击的原理。正常的网络通信过程中，连接在同一个交换机上的主机 A、B 都通过路由器(网关)访问 Internet。图 1-19 说明了主机 A 对 B 的攻击过程。主机 A 将网关的 IP 地址及 A 的 MAC 地址以 ARP 响应包的形式发给 B，让 B 误以为网关在 A 这里，此时所有 B 对 Internet 的访问请求都会先到达 A，然后转发给网关。同时，主机 A 将 B 的 IP 地址及 A 的 MAC 地址以 ARP 响应包的形式发送给网关，让网关误以为 B 在 A 这里，此时所有网关返回给 B 的数据都会先到达 A，再由 A 转发给 B。

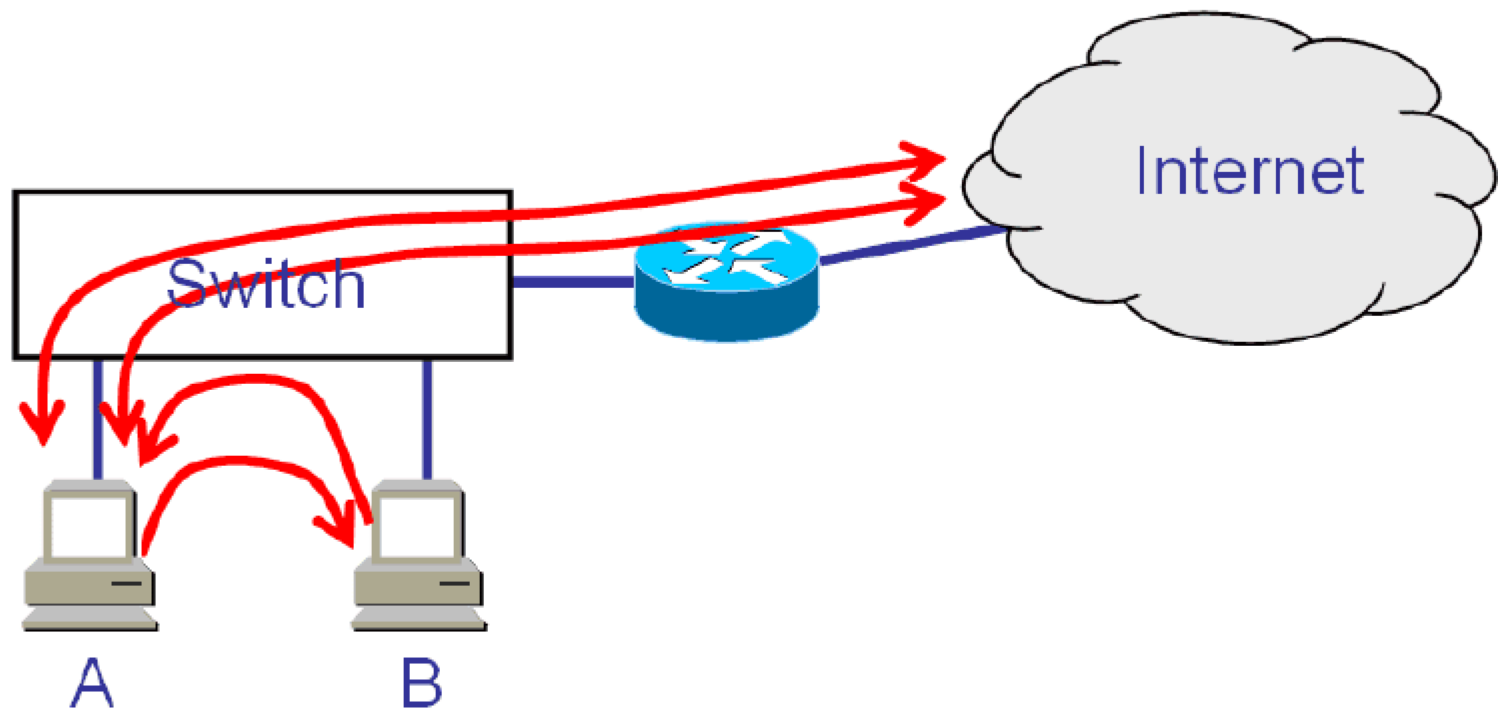


图 1-19　利用 ARP 欺骗实现中间人攻击

对普通用户而言，防范 ARP 欺骗可行的办法是，在网络正常时，记下网关的 MAC 地址，设置一条静态 ARP 缓存表项，此表项不会被 ARP 响应数据包更新。然而，要从根本上杜绝 ARP 欺骗对用户计算机及网络环境造成的影响，需要支持防范 ARP 攻击的交换机，结合相应的安全策略，才能有良好的效果。

1.3.3　传输层协议

TCP/IP 体系的传输层提供了两类服务：可靠传输服务(TCP 协议)及不可靠传输服务(UDP 协议)。TCP 是面向连接的服务，用 TCP 通信，首先必须建立连接，并且在传输过程中，协议机制能保障数据按发送顺序可靠到达目的地。TCP 协议适合传输对可靠性要求高、连续的大量数据。TCP 连接的建立、释放过程都需要一定的开销，如果频繁建立、释放连接，会导致传输效率显著降低。UDP 是无连接服务，通信前无须建立连接，任何时候只需直接将数据发出即可。UDP 灵活、方便，不存在连接管理问题，适合传输间断、小块数据。UDP 提供的是一种不可靠的传输服务，如传输中数据出现丢失、乱序的问题，UDP 都不会做处理。

TCP、UDP 分别适应不同的应用场合，当需要传输连续、数据量很大、对可靠性要求高的数据时，应采用 TCP 协议，而在需要传输大量离散数据，且对可靠性要求不太高时，则适合用 UDP 协议。

基于网络层编址、寻址(即路由)功能，数据能从一台主机到达网络中任意其他主机，单数据到达目的主机后，由目的主机的哪个应用程序来处理，则不是网络层协议所能解决的，也就是说，网络层实现的是主机端到端的传输能力。网络数据的发送、接收，最终都必须由特定的应用程序来完成，因此，必须引用新的机制，来实现网络数据与应用程序的关联，这就是传输层的端口(Port)所要做的，所以说，传输层提供的是应用程序端到端的传输能力。

端口，是一个 16 比特的数字，故端口号的最小值为 0，最大值为 65 535。其中，0～1023 称为熟知端口(Well-Known Port)，熟知端口通常用于关联常用的网络服务。例如，80 端口常用于关联 Web 服务，以提供网页浏览服务；53 端口常用于关联 DNS 服务，以提供域名解析服务。需要注意的是，因为 TCP/IP 的网络层提供了两套服务——TCP 和 UDP，因此对应就有两套端口机制。也就是说，TCP 有一套端口，从 0 到 65 535，同样 UDP 也有一套端口，从 0 到 65 535。在一些需要严密表述的场合，仅指出端口号是不够的，还应当指明是 TCP 端口还是 UDP 端口。前文所述 Web 服务的 80 端口，是指 TCP 的 80 端口，而 DNS 服务的 53 端口，通常是指 UDP 的 53 端口。

IP 地址、端口用“：”连接起来，称为套接字(Socket)，用于描述一个网络应用程序的附着点，如“192.168.1.1:80”。进行通信的两个应用程序，在发送接收数据之前都需指明协议类型，即是 TCP 协议还是 UDP 协议，然后设定好源套接字、目的套接字，才能开始数据传输。采用 TCP 协议进行通信的一对套接字，称为一个 TCP 连接。UDP 是无连接服务，故不存在 UDP 连接的概念，虽然 UDP 通信也需要一对套接字。已建立的 TCP 连接实例见图 1-20，其中演示了查看包含 TCP 连接在内的当前网络状况的命令 netstat，此命令适用于 Windows 系统及 UNIX/Linux 系统。netstat 命令的参数-a 表示显示所有连接和监听端口，参数-n 表示以数字形式显示 IP 地址和端口号(无此参数则会以主机名/域名的方式显示 IP，以服务名的方式显示熟知端口号)，-o 参数仅适用于 Windows XP 及 Windows 2003 以上的操作系统，表示在显示连接及端口监听状态的同时，还显示使用此连接或监听端口的进程 ID，并以 PID(Process ID，进程 ID)的方式列出。

在 TCP 连接建立过程中，等待连接的一方称为服务端，其特点是特定的某个 TCP 端口处于监听(Listening)状态，即该 TCP 端口始终处于开放状态。发起连接的一方称为客户端，其相应的 TCP 端口仅在连接发起的时候才打开，且发起连接方的 TCP 端口若非特意指定，均由系统自动分配。因 0～1023 端口为熟知端口，故发起连接方的 TCP 端口范围通常为 1024～65 535。

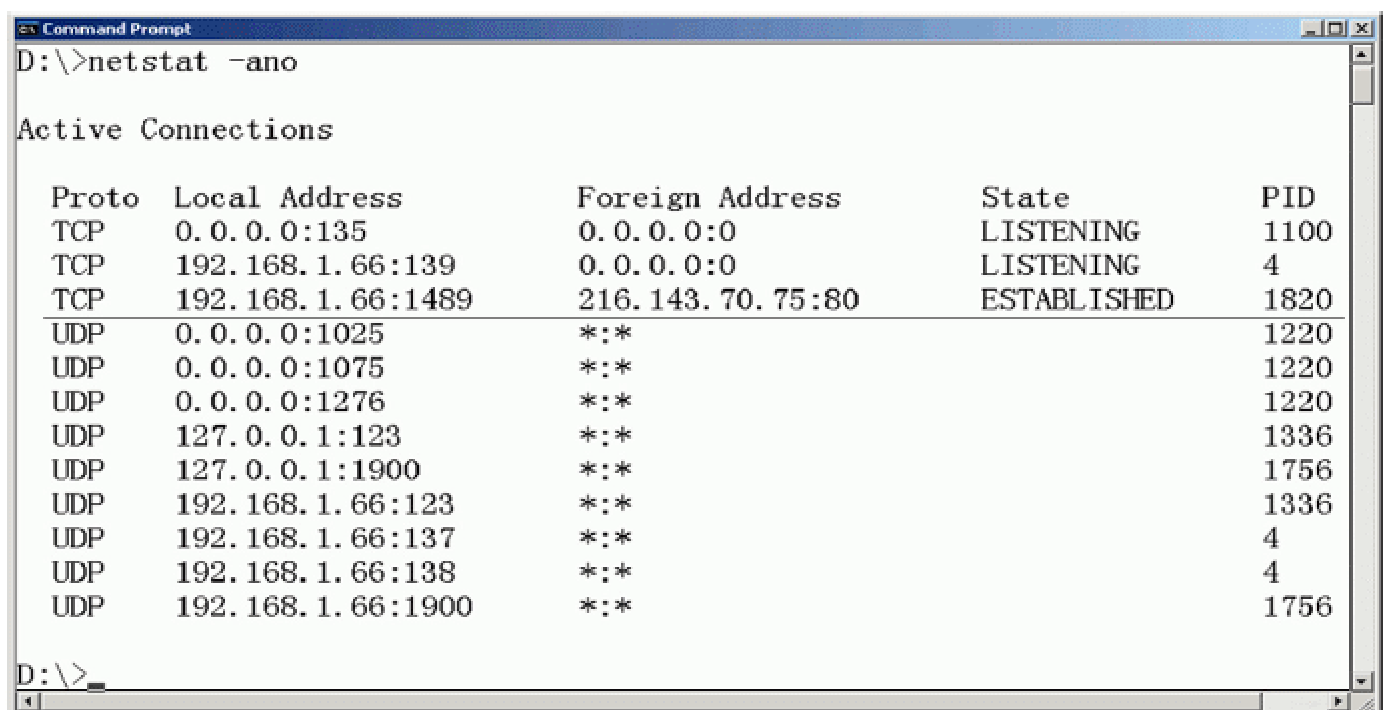


图 1-20　TCP 连接实例

TCP 连接的建立，需要由称为“三次握手”的三个 TCP 报文段(TCP Segment)来实现，如图 1-21 所示。客户端首先打开一个用于建立连接的端口，然后向服务端的特定端口发送一个包含 SYN 标记(表示连接建立请求)的报文段，若服务端的相应端口处于监听状态，则向客户端返回一个包含 SYN 和 ACK 标记的报文段，ACK 标记表示确认客户端的连接请求，正常情况下，客户端再向服务端发送一个包含 ACK 标记的报文段，以通知服务端当前连接已被客户端确认。

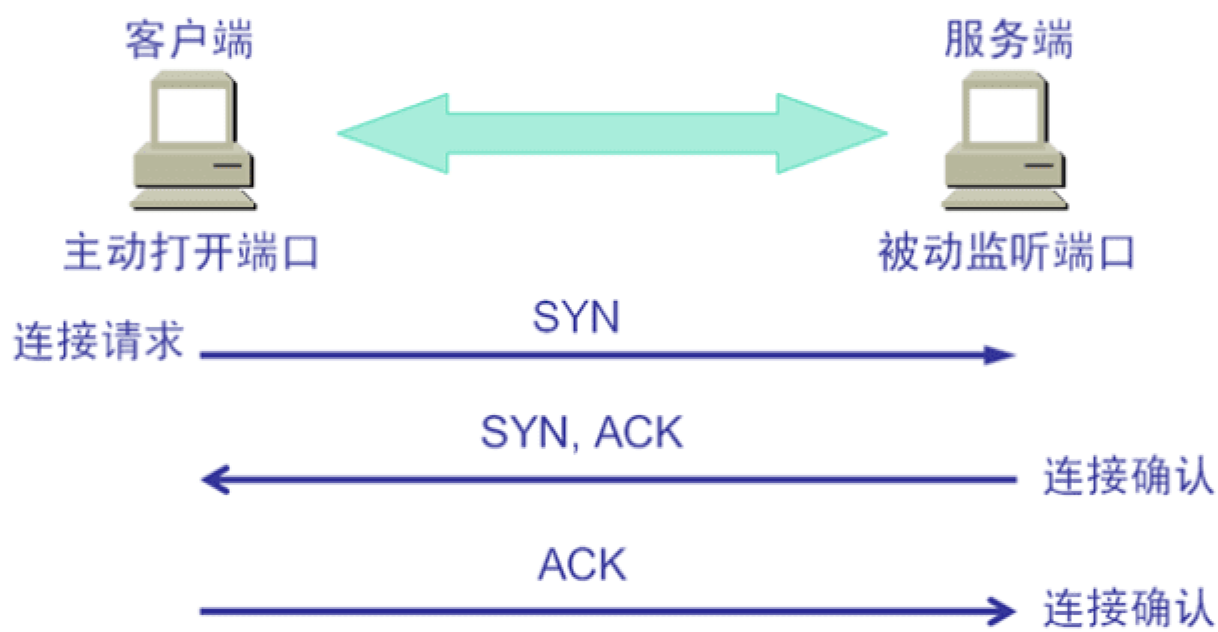
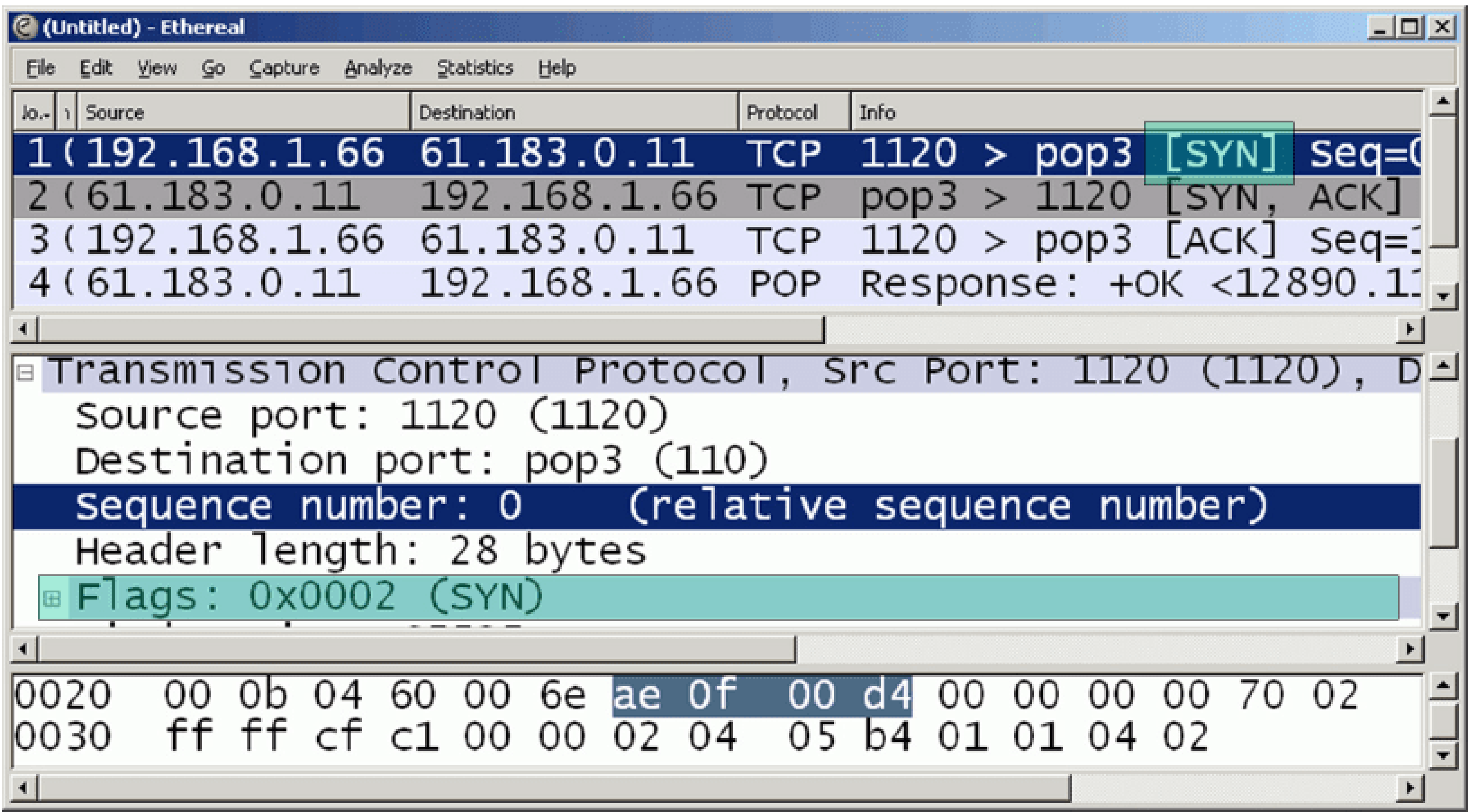
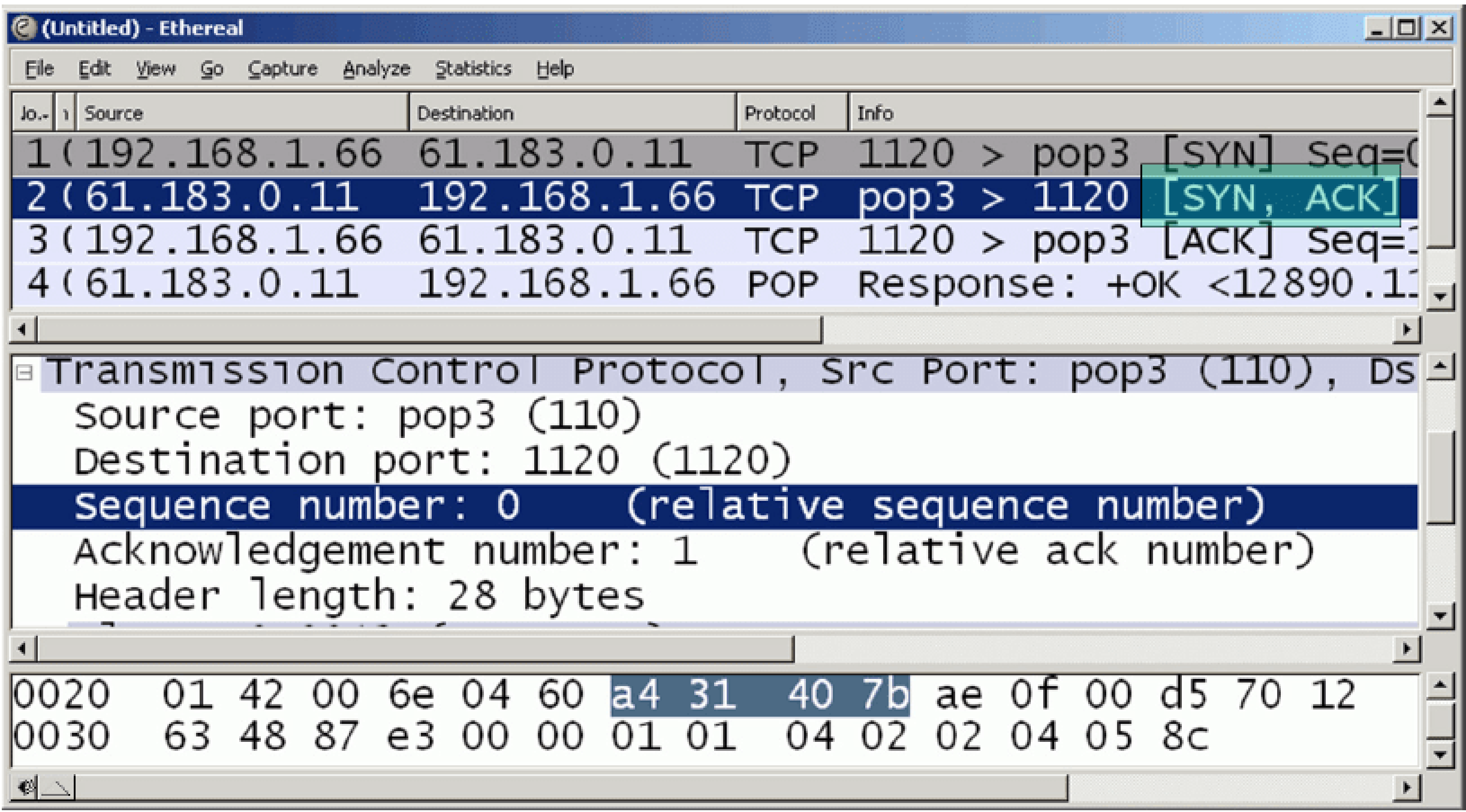


图 1-21　TCP 三次握手

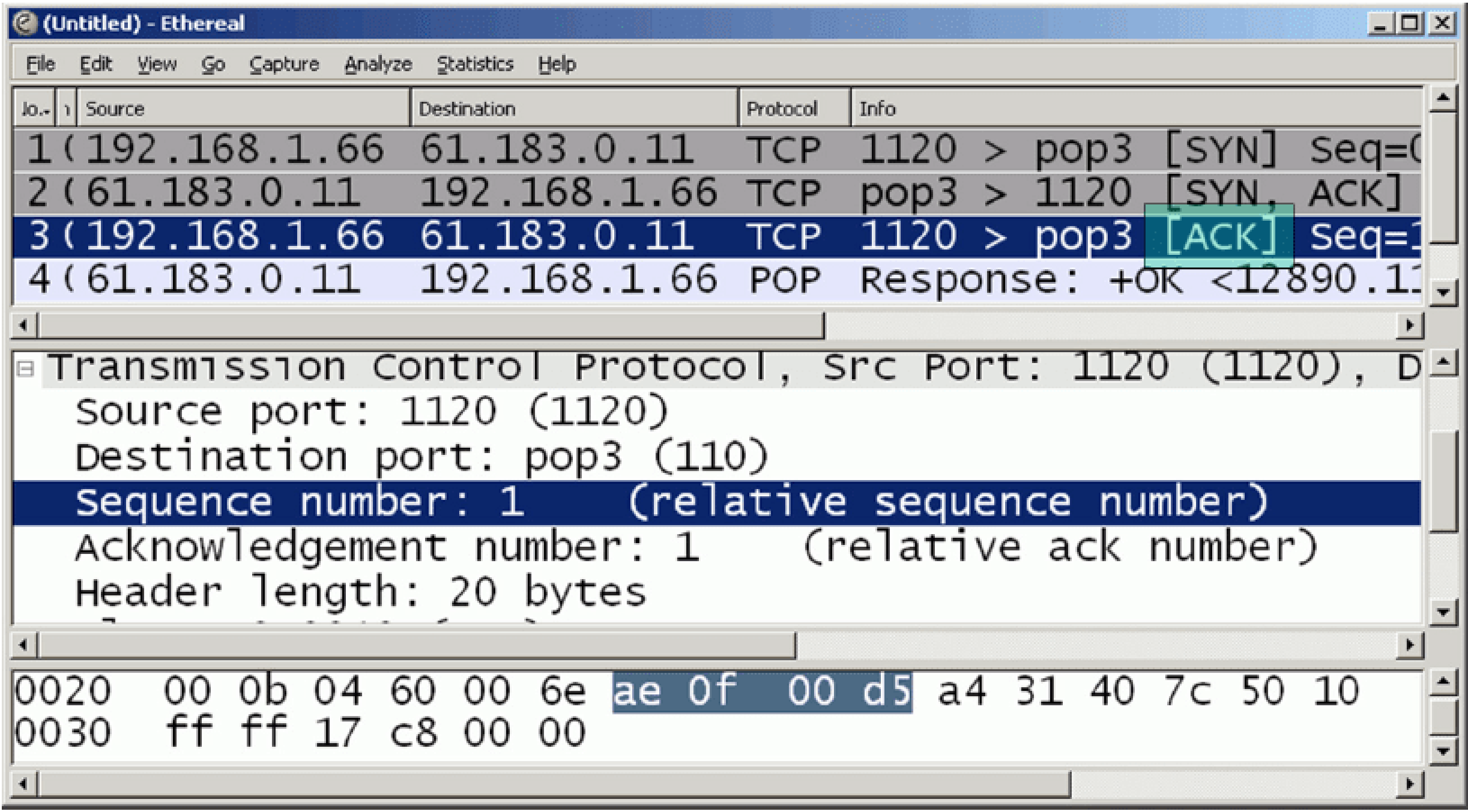
图 1-22 展示的是一次 TCP 连接建立过程中捕获到的 TCP 报文段数据。源主机 IP 为 192.168.1.66，目的主机 IP 为 61.183.0.11，连接的目的端口是 POP3 协议所用的 110(TCP)端口，POP3 协议是电子邮件系统收信时使用的协议，当使用电子邮件客户端程序(如 Outlook Express 等)向邮件服务器收取信件时，使用的就是此协议。



(a)



(b)



(c)

图 1-22　TCP 三次握手对应的 TCP 报文段

注意观察图 1-22 中，在 TCP 连接的建立过程，每个 TCP 报文段所包含的 SYN、ACK 标记在灰色区域。要想深入了解协议的工作细节，可对此报文段的其他字段进行细致分析。

TCP 连接的释放过程与建立过程类似，也是通过三个 TCP 报文段来实现的，区别在于连接建立时使用的是 SYN 标记，释放时使用的是 FIN 标记。

根据 TCP 三次握手建立连接的过程可知，对于服务端而言，在向客户端发送确认连接的 ACK 报文段后，还要等待客户端返回的 ACK 报文段，以完成 TCP 连接。在等待客户端返回 ACK 报文段时，服务端必须分配一定的资源，用于这个预期的 TCP 连接。基于此过程，恶意用户可伪造源 IP 地址，向服务端发起 TCP 连接请求，服务端向伪造的源 IP 返回 ACK，并等待其确认，此时的 TCP 连接状态称为半连接。因伪造的源 IP 根本没有发送过连接请求，或者伪造的 IP 根本就不存在，因而服务端会一直等待三次握手中最后这个 ACK 报文段，直至超时。在此过程中，服务端因此而分配的资源(CPU、内存等)会一直被占用。当恶意用户向服务端大量发送这类伪造源 IP 的 TCP 请求时，就会导致服务端的资源被过度消耗，最终无法为普通用户的合法 TCP 请求分配资源。这种利用大量 TCP SYN 报文对服务器进行攻击的方式称为“SYN Flood”，是典型的拒绝服务(DoS，Denial of Service)攻击。因为 TCP/IP 体系在设计之初缺乏足够的安全机制，SYN Flood 虽然原理简单，但攻击危害大，且较难彻底解决。

1.3.4　应用层协议

应用层提供了丰富多样的各类应用服务，典型的应用层协议有 DNS、HTTP、FTP、SMTP、POP3 等。

DNS(Domain Name Service，域名服务)是一种命名系统，提供由 IP 地址到域名，或由域名到 IP 地址的解析服务。网络通信最终都是以 IP 地址来识别不同计算机，但 IP 是一串数字，难于理解和记忆。DNS 系统可为 IP 地址分配一个(或多个)易于记忆的中英文字符串，即 IP 地址对应的域名。已知域名求 IP 地址的过程称为正向解析，已知 IP 地址求域名的过程称为反向解析。通常情况下，使用频率较高的是正向解析过程。当 DNS 服务器出现故障时，用户的网络其实并没有中断，但普通用户会感觉很多网站都打不开，因为大多数情况下用户是以域名的方式来访问目标网站的，DNS 服务器的故障会导致目标网站的域名不能解析，因而无法访问，如果直接使用 IP 来访问目标网站，则基本不受此影响。因此，用户对网络的正常访问，严重依赖于 DNS 服务器的正常运转。

2009 年 5 月份国内十多个省份出现的网络故障，主要原因就是著名的国产流氓软件“暴风影音”包含的恶意软件发出大量非正常 DNS 解析请求，导致部分电信 DNS 服务器瘫痪，从而导致大面积用户域名解析异常。图 1-23 是在某台 DNS 服务器上捕获到的网络数据，图中第二列是时间，以秒为单位。由图可见，在极短的时间内，暴风影音所包含的恶意软件发出了大量目标域名为“sandai.net”、“baofeng.com”的 DNS 解析(QUERY)请求，正常的数据包所占比例很少。这个例子中的数据是在一个仅数百台在线主机的网络中捕获到的，如果网络规模更大，暴风影音所产生的这些垃圾网络通信数据的危害更严重。

自 1990 年起，HTTP(Hypertext Transfer Protocol，超文本传输协议)就已经被应用于 WWW(World Wide Web，万维网)。HTTP 目前依然是 Internet 上应用最为广泛的应用层协议，它是一种请求/响应式的协议。客户机与服务器建立 TCP 连接后，发送一个请求给服务器；

服务器接到请求后，给予相应的响应信息。HTTP 的第一版本 HTTP 0.9 是一种简单的用于网络间原始数据传输的协议，HTTP 1.0 由 RFC(Request For Comments，请求注解，Internet 标准草案)1945 定义，在原 HTTP 0.9 的基础上，进行功能扩充。后续版本 HTTP 1.1(RFC 2616)的要求更加严格，以确保服务的可靠性，增强了在 HTTP 1.0 没有充分考虑到分层代理服务器、高速缓冲存储器、持久连接需求或虚拟主机等方面的功能。安全增强版的 HTTP(即 S-HTTP 或 HTTPS)，则是 HTTP 协议与 SSL(Security Socket Layer，安全套接字层，详见后续章节的介绍)的结合，使 HTTP 的协议数据以加密的方式传输，避免明文协议数据出现，以保障传输数据的安全。

80	00.000825	DNS	C QUERY NAME=hub5u.sandai.net
81	00.000484	DNS	C QUERY NAME=hub5pn.sandai.net
80	00.002462	DNS	C QUERY NAME=hub5u.sandai.net
81	00.011065	DNS	C QUERY NAME=hub5pn.sandai.net
81	00.001563	DNS	C QUERY NAME=hub5pn.sandai.net
78	00.010719	DNS	C QUERY NAME=ebvezjpctr.biz
131	00.004405	TCP	Src= 4477,Dst= 3721,.AP...,S=20757709
76	00.003569	DNS	C QUERY NAME=cdukqrrqo.ws
85	00.015859	DNS	C QUERY NAME=videodown.baofeng.com
80	00.000773	DNS	C QUERY NAME=live.baofeng.com
85	00.001796	DNS	C QUERY NAME=videodown.baofeng.com
85	00.000077	DNS	C QUERY NAME=videodown.baofeng.com
80	00.000071	DNS	C QUERY NAME=live.baofeng.com
80	00.000459	DNS	C QUERY NAME=hub5u.sandai.net
80	00.001109	DNS	C QUERY NAME=hub5u.sandai.net
81	00.001037	DNS	C QUERY NAME=hub5pn.sandai.net
81	00.000663	DNS	C QUERY NAME=hub5pn.sandai.net
81	00.023414	DNS	C QUERY NAME=hub5pn.sandai.net

图 1-23　“暴风影音”所含恶意软件产生的垃圾网络通信数据

HTTP 协议和 Web 站点、Web 页面、Web 浏览器、Web 服务器间的关系如图 1-24 所示。

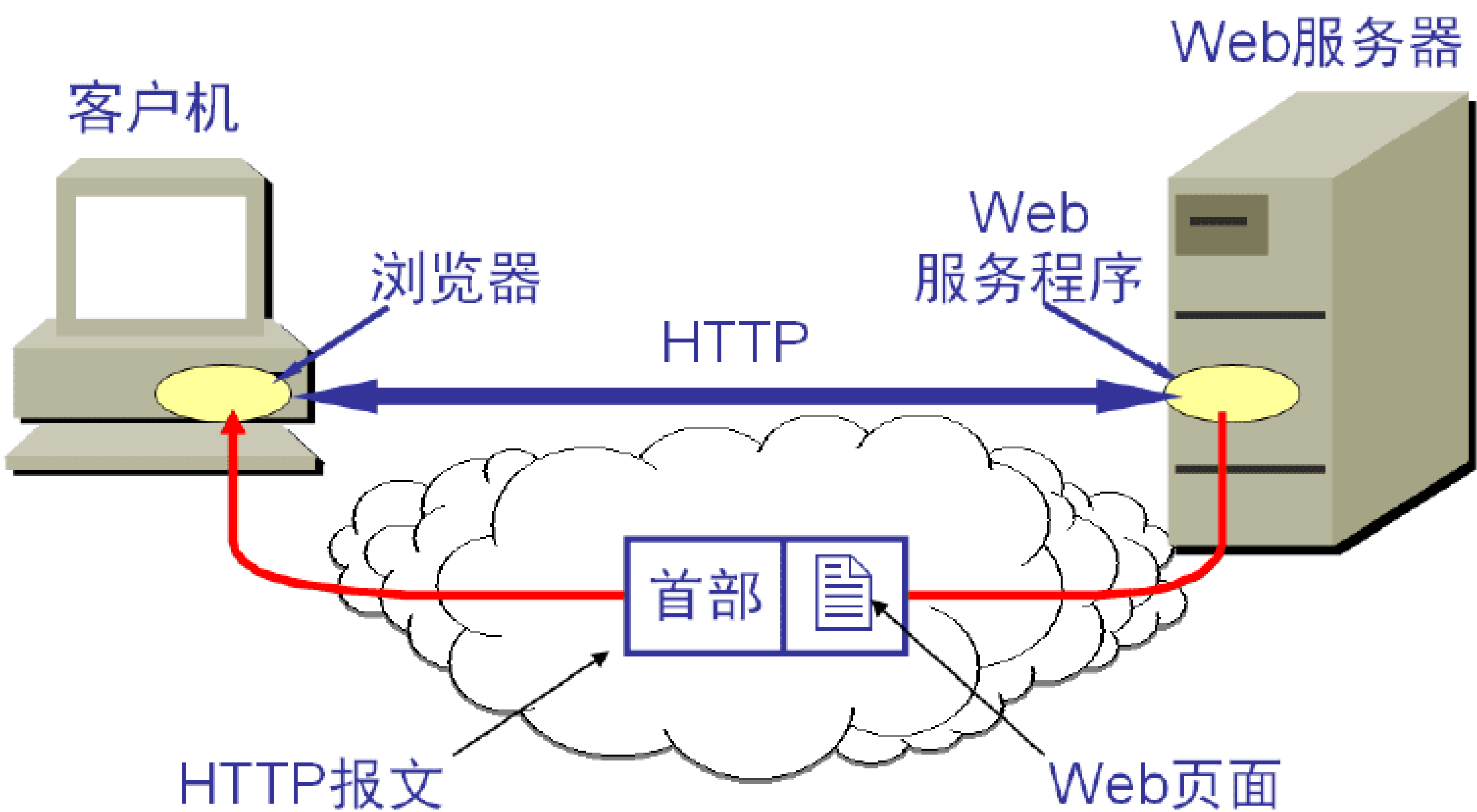


图 1-24　Web 页面和 HTTP 协议的关系

Web 服务器是运行 Web 服务程序的计算机，用户要浏览 Web 站点，必须在 Web 浏览器(如 Internet Explorer、Firefox 等)中输入运行着 Web 服务程序的计算机的域名或 IP 地址。浏览过程中，Web 浏览器是客户端程序，向 Web 服务程序发出浏览请求，Web 服务程序根据请求内容将存放在 Web 服务器上的 Web 页面封装成 HTTP 协议报文的格式，返回给 Web 浏览器。在 Web 服务器上，一系列 Web 页面以及相关的图片、视频等其他媒体的集合，即称为 Web 站点。

一次典型的 Web 页面浏览过程所产生的网络通信如图 1-25 所示。由图可知，请求的 Web 页面返回给客户端后，客户端和服务器间的 TCP 连接即被释放。下次客户端再和服务器联系时，服务器无法判断客户端的身份，也就是说，服务器不能区分曾经访问过它的那些客户端，这称为 HTTP 协议的无状态(Stateless)特性。HTTP 协议的无状态特性在许多需要身份验证的 Web 站点中显然是不能满足要求的，不可能要用户每访问一个页面就输入一次用户名、密码。为了解决这个问题，HTTP 协议扩充了两种机制，以保留曾经登录过的用户身份。第一种机制是在 HTTP 请求报文加入一个头部选项"Connection：Keep-Alive"，包含此选择后，客户端和服务器间的 TCP 连接在页面返回后不会立即释放，而是经历一个超时(Time Out)值后才释放，在超时时间范围之内，一直保持 TCP 连接状态。Keep-Alive 的超时时间受客户端、服务端双方的影响，取值为两者中小的那个，通常为 60 秒。另一种普遍使用的机制是 Cookie。Cookie 以文件的形式保存在客户端，每次客户端向服务器发送请求时，都会读取相应 Cookie 文件，并把相关信息填写到 HTTP 请求报文的头部。有了 Cookie 机制，用户只需登录一次，将服务器返回的身份信息(通常为加密的形式)写入到 Cookie 文件中，后续对 Web 服务器的访问时，此身份信息都被附加在请求报文中，服务器检查后即可验证此用户的身份。

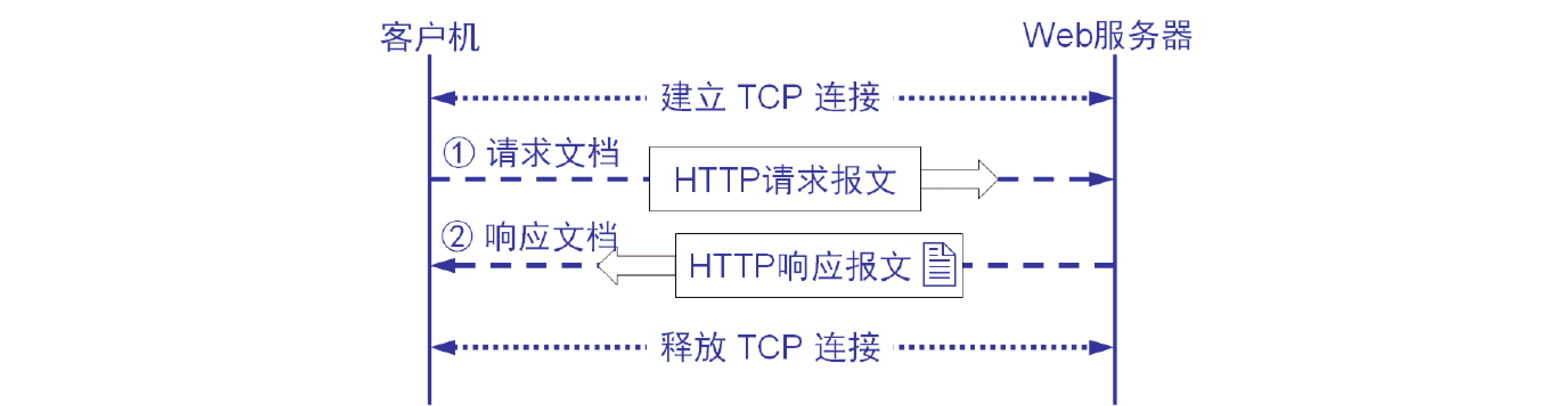


图 1-25　Web 页面浏览过程

在浏览 Web 站点时，访问同样的地址，若每次返回相同的 Web 页面，则此页面称为静态页面；若根据访问的时间、参数不同，返回的 Web 页面也不同，则此页面称为动态页面。动态页面每次返回不同结果，是因为有程序在浏览器(客户端)或服务器(服务端)上运行，该程序根据用户请求的时间、参数，以及程序的流程，将不同的结果呈现给浏览器。

FTP 是 Internet 上以 C/S(Client/Server，客户端/服务器)方式处理文件的协议。客户端可以向服务器上传文件，也可以从服务器下载文件，且上传、下载动作都支持续传，即传输中断后，下次传输可从中断点继续进行，以避免重复传输。

应用 FTP 进行文件传输需要用到两个 TCP 连接：控制连接和数据连接。控制连接用于传递控制命令、操作状态信息，当客户端登录到 FTP 服务器后，控制连接始终存在，客户端从 FTP 服务器登出时才释放控制连接。数据连接用于传递非控制命令的数据，比如列目录操作、文件上传下载操作，数据连接仅当传递数据时存在。例如，用户登录到 FTP 服务器后，下载了 10 个文件，然后退出登录，则此过程中，建立、释放一个控制连接，而每传输一个文件，都会建立、释放一个数据连接，总共建立、释放 10 个数据连接。由前文所述，TCP 连接的建立、释放，都需要一定的开销，故当有大量小文件需要传输时，FTP 协议针对每个文件都进行 TCP 连接的建立释放操作会造成大量开销，从而严重影响传输效率。因此，当传输

的文件数量很多且文件尺寸普遍较小时，应该将众多小文件打包成单个大文件，再通过 FTP 传输，这样能带来传输效率的显著提升。

需要注意的是，FTP 协议在工作时，控制连接都是由客户端向服务器发起的 TCP 连接，但数据连接的方向则有两种可能。若数据连接是由服务器向客户端发起的 TCP 连接，则这种工作模式称为主动模式(Active Mode)。若数据连接是由客户端向服务器发起的，则这种工作模式称为被动模式(Passive Mode)。可见“主动”、“被动”都是以服务器的视角来观察的，服务器主动发起连接则为主动模式，被动等待连接则为被动模式。实际网络环境中，很多时候客户端处于内网，或者受防火墙的保护，此时主动模式常常无法工作，因为服务器向客户端发起的连接到达内网边界或防火墙边界时会被阻断，连接无法建立。内网用户或防火墙保护下的用户向外发起 TCP 连接通常不会被阻止，因此这种情况下可以使用被动模式，由客户端向服务器发起数据连接。FTP 主动模式、被动模式工作原理见图 1-26，其中 x.x.x.x 表示 IP 地址。由图可知，控制连接服务器端的端口默认均为 21(TCP)。主动模式下服务器端的数据连接端口为 20，而被动模式下服务器端的数据连接端口不确定，和 FTP 服务程序的设置有关。

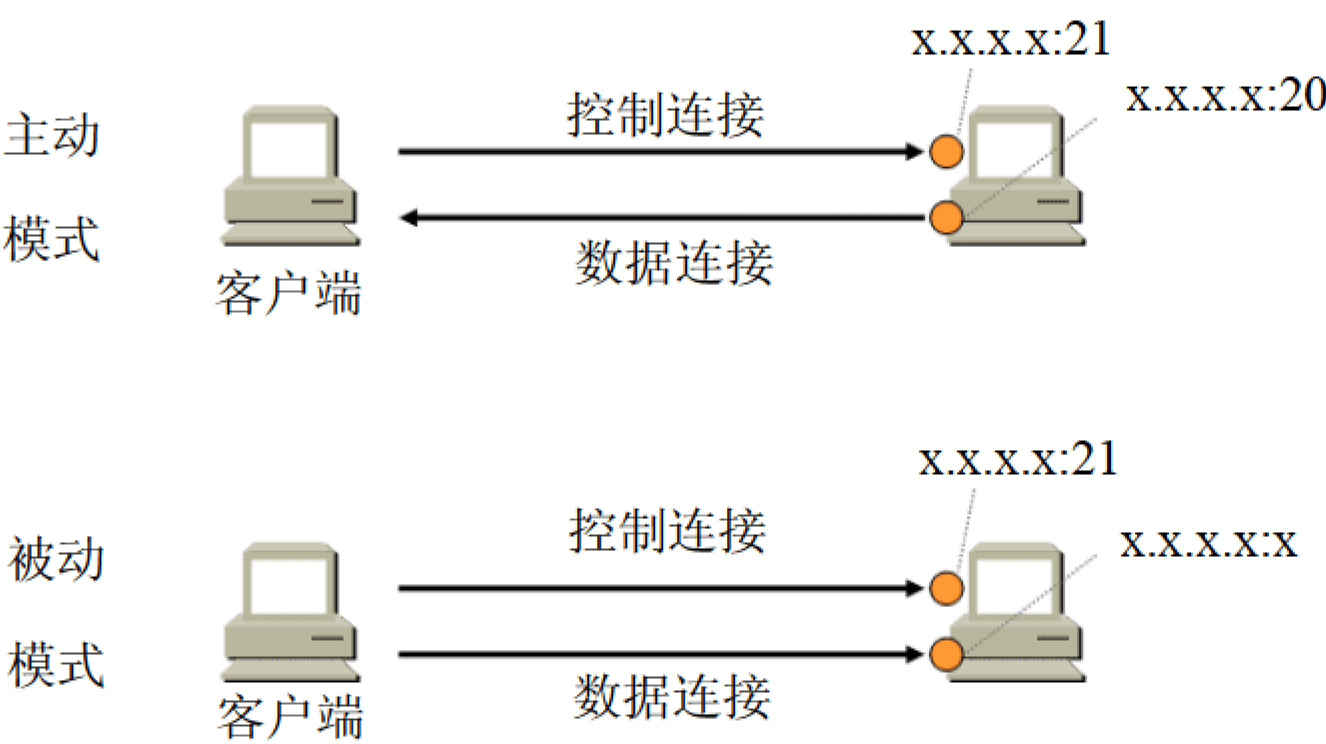


图 1-26　FTP 主动模式、被动模式工作原理

Internet 中电子邮件系统的工作流程、原理，完全是仿照现实生活中的邮局系统而来的。电子邮件的发送过程，就好像某人走到邮局去发送包裹，网络中的这个过程使用的协议称为 SMTP(Simple Mail Transfer Protocol，简单邮件传输协议)。SMTP 服务器端使用的是 TCP 25 端口。邮局系统发出的包裹通过若干个邮局中转，最后到达收件人所在的邮局，此时，收件人需要到邮局去取回包裹。电子邮件系统中的邮件接收过程也与此一致，使用的协议称为 POP3(Post Office Protocol 3，邮局协议版本 3)。POP3 协议服务端使用的默认端口是 TCP 110。早期的电子邮件系统只能传输文本信息，通过对协议进行扩充，任意格式的媒体文件都可编码后通过电子邮件系统传输。网络中的用户通过电子邮件传输文件的主要好处在于，用户双方无须同时在线，并且每个人可以拥有自己的一块私有存储区域。

1.4　相关的基本概念

PDU(Protocol Data Unit，协议数据单元)是各协议层所处理数据的基本单位，协议层次不同，PDU 的称谓、格式均不相同。物理层的 PDU 是二进制位(Bit)，链路层的 PDU 是帧，网

络层的 PDU 是 IP 数据包(Packet)，传输层的 PDU 是报文段(Segment)，应用层的 PDU 是报文(Message)。

根据网络设备所能识别、处理的数据所处的协议层次，不同的网络设备被称为一层设备、二层设备、三层设备、四层设备或七层设备。这里所说的“某层”指的是 OSI 七层模型中的层次。对这些设备的称谓常见的有二层交换机、三层交换机、四层交换机或七层交换机。一层设备只能处理物理层的数据，即将所有线路上的二进制“1”、“0”进行信号放大、整型后输出，典型的一层设备是中继器(Repeater)。二层设备能识别链路层数据——帧，并根据帧内的源地址、目的地址来判断对数据如何处理。例如，日常使用的以太网交换机(Switch)多数都是二层交换机，根据收到的以太网帧内的 MAC 地址，来判断将帧转发到哪些端口。三层设备能对网络层的 IP 数据包进行分析，根据 IP 数据包中包含的目标 IP 地址进行不同的处理，Internet 上的路由器是典型的三层设备，路由器根据 IP 数据包的目标地址进行路由选择，决定 IP 数据包应该走哪条路径从而到达目的地。四层设备在能解析网络层 IP 数据包的基础上，还能识别传输层的端口号。七层设备则能对应用层协议进行分析，根据分析结果对数据进行过滤、加工等处理。

由图 1-15 可知，帧的有效载荷数据区最多能包含 1500 字节，称为 MTU(Maximum Transfer Unit，最大传输单元)，由于上一层的 PDU－IP 数据包整个都被封装在链路层帧的数据区，因而单个 IP 数据包的最大长度即为 1500 字节。IP 数据包分为头部和有效载荷数据区，头部长度为 20 字节，故 IP 数据包的数据区最大长度为 1500－20＝1480 字节。若网络层有超出 1480 字节的数据需要发送，则需要将数据以 1480 为单位，分为多个 IP 数据包发送，这个过程称为 IP 数据包分片(Fragmenting)，分割后的多个片断送给链路层后，再封装成多个帧。需要强调的是，数据发送过程中 IP 数据包分片的动作在网络层进行，但到达目的地后，各片断的合并操作是在传输层进行的，网络层不保证各片断按分片前的次序到达目的地。

本 章 小 结

本章主要介绍了计算机网络的基础知识，包括：计算机网络发展历程；两种网络体系结构的基本概念；从 TCP/IP 协议体系的低层的链路层到高层的应用层，介绍了各层的基本功能，以及基本运行机制、工作原理；最后介绍了计算机网络相关的几个基本概念。

课 后 练 习

一、 填空题

1. TCP/IP 协议模型中，物理层定义物理接口的机械、电气等特性，(　　　　　　)层将待传输的比特流划分成帧，(　　　　　　)层完成 IP 数据包的路由选择。

2. 在网络中，物理层传输的数据单位称为比特，数据链路层传输的数据单位通常称为

(　　　　　)，网络层传输的数据单位通常称为(　　　　　)。

3. 用于测试到目标主机的网络是否通畅最常用的命令是(　　　　　)。

4. 一个 TCP 连接的建立，需要由(　　　　　)次“握手”来完成。构成 TCP 连接的一对套接字，由 IP 和(　　　　　)组成。

5. MAC 地址是分层网络模型中(　　　　　)层的地址，MAC 地址通常又称为(　　　　　)地址或硬件地址。

二、 选择题

1. 当前主要使用的 TCP/IP 协议中，其 IP(v4)协议子网掩码的长度为(　　)。

A. 4　　B. 16　　C. 32　　D. 128

2. 子网掩码中，1 和 0 分别代表 IP 地址中对应位为(　　)。

A. 子网号 子网号　　B. 子网号 主机号

C. 主机号 子网号　　D. 主机号 主机号

3. 在 IP 地址的分类中，(　　)IP 地址可容纳的主机数量最多。

A. A 类　　B. B 类　　C. C 类　　D. D 类

4. DoS 攻击中的 DoS 是(　　)的缩写。

A. Disk Operation System　　B. Do it of Self

C. DOS System　　D. Denial of Service

5. TCP 协议提供的服务属于(　　)类型。

A. 无连接　　B. 分段　　C. 面向连接　　D. 以上都是

三、 简答题

1. 网络体系结构包含哪三个方面的内容？
2. 在发送过程中，数据在各层协议间的关系如何？
3. 为何传统以太网的数据帧的最大长度为 1518 字节？
4. FTP 协议中的两个连接分别是什么？FTP 文件传输的两种模式分别是什么？
5. 网络设备中，何谓二层设备？

第2章　网络安全基础

随着信息化的浪潮席卷全球，当今世界正经历着以计算机网络为核心的信息革命，信息网络逐步成为社会的神经系统，并将彻底改变人类传统的工作、生活方式。

经过几十年的迅速发展，计算机网络不再局限于最初的局域网(Local Area Network，LAN)，已跨过城市、国家和地区的范围，实现了网络扩展与异构网互联，形成更广泛意义上的互联网络，即广域网(Wide Area Network，WAN)。这种趋势使得计算机网络深入到科研、文化、教育、经济与国防建设的各个领域，推动了整个社会的信息化发展。同时，这种发展也带来了一些负面影响及问题：网络的开放性增加了网络安全的脆弱性和复杂性；信息资源的共享和分布处理增大了网络受到非法攻击的可能性；网络内各种不同类型的计算机系统存在的安全漏洞被不法之徒利用，借以入侵计算机，获取或篡改重要数据；人为或自然因素造成对计算机网络信息安全的威胁。这一系列问题，使得网络安全成为计算机网络技术人员长期需要面对和解决的重大问题。

本章重点

- 网络安全概述
- 网络面临的安全威胁
- 网络安全需求分析
- 网络安全模型
- 网络安全体系结构

2.1　网络安全概述

计算机网络安全不仅包括组建网络的硬件、管理控制网络的网管软件，也包括网络内共享的资源、快捷的网络服务，所以定义网络安全应考虑涵盖计算机网络所涉及的所有内容。参照国际化标准组织(ISO)给出的定义，我们认为计算机网络安全是指：“保护计算机网络系统中的硬件、软件和数据资源不因偶然或恶意的原因遭到破坏、更改、泄露，使网络系统连续可靠性地正常运行，网络服务正常有序。”

2.1.1　网络安全发展历程

最初，因特网(Internet)尚未出现，计算机网络未成型，人们使用普通邮件或电话进行交

流，紧急情况下可以发送电报进行通信。随后，网络和 Internet 使得这一切发生了天翻地覆的变化。Internet 起源于 1969 年初建立的 ARPANET(Advanced Research Projects Agency Network)：一个非常小的、独立封闭的、监管严格的网络。它是美国国防部高级研究计划管理局为准军事目的而建立的，开始只有 4 台主机，这就是只有 4 个节点的“网络之父”。到 1972 年公开展示时，由于一些学术研究和政府机构的加入，ARPANET 网络已经连接了 50 所大学和研究机构的主机；到 1982 年，ARPANET 实现了与其他多种异构网络的互联，从而形成了以它为主干网的互联网。

1983 年，美国国家科学基金会(National Science Foundation，NSF)出巨资，建造了全美五大超级计算机中心。为了使全国的科学家、工程师能共享超级计算机的资源，又建立了基于 IP 协议(Internet Protocol)的计算机通信网络 NFSNET。1986 年，NFSNET 建成后取代 ARPANET 成为互联网的主干网。发展到 1996 年，已经连接了世界上 195 个国家，遍布每个大洲(甚至南极洲)的 1300 多万台计算机。如今，它已经成为世界上最大的计算机互联网络，连接了全球不计其数的网络与计算机，同时也是世界上最为开放的网络系统，允许世界上数以亿计的人们进行通信和信息共享。

互联网在赋予用户丰富的资源共享、高度开放性和跨地区跨时间的自由性的同时，也使得随之暴露出来的网络安全问题日趋严重。病毒与病毒防治，入侵和安全防范的较量，此消彼长，正所谓“魔高一尺，道高一丈”，注定了这将是一场长期艰巨的战争。作为计算机专业人士，特别是有志于网络安全方面的研究人员，知己知彼方能百战百胜，意思就是熟悉敌人才能有针对性地提高自己，更加有把握战胜敌人。网络安全的工作实际上就是发现、了解问题，并根据具体情况作出适当的反应，研究出解决问题的技术和手段并加以应用，做好安全防范措施以杜绝类似安全问题的再次发生。从某种意义上来说，网络安全的发展历史，就是一部与破坏性病毒和网络非法入侵的斗争史。下面，通过回顾历史上一些比较有影响力的网络安全事件，以更好地了解信息网络系统的安全发展历程。

1. 网络安全历史事件

回溯到 20 世纪 80 年代。1987 年，病毒“维也纳(Vienna)”问世，拉尔夫 • 伯格(Ralph Buerger)将其分解并发表在他的著作《计算机病毒：一种高科技疾病》(Computer Viruses:a High-tech Disease)。这本书阐述了如何编写和实现繁衍成百上千的计算机病毒的概念，使得编写计算机病毒成为一种时尚。1988 年 11 月 2 日，美国航天局艾姆斯研究中心(NASA Ames Research Center)的彼得 • 伊(Peter Yee)在互联网邮件列表里发布信息：“我们正在遭受因特网病毒的攻击！”这个报告成为了后来为人熟知的莫里斯蠕虫病毒(Morris Worm)发作的第一份历史记载。罗伯茨(Roberts)，一名 23 岁康奈尔大学(Cornell University)的在校学生编写了此代码作为研究课题的一部分，旨在检测因特网的大小。由于代码里的一个瑕疵，导致该程序利用 UNIX 的弱点并快速传播，感染了成倍增长的计算机最终导致它们瘫痪。1989 年 10 月，手淫蠕虫(Worms Against Nuclear Killers，WANK worm)，一个自动攻击 VMS 系统的蠕虫病毒出现，肇事者至今未明，成为有记载的史上第一次网络犯罪悬案。

20 世纪 90 年代，各种病毒变种和入侵手段进一步升级。1990 年，一种多态性的病毒：“特奎拉”(Tequila)病毒出现，该病毒能对自身特征进行修改，从而避免反病毒程序的检测，

1994 年 4 月 11 日该病毒全面爆发。1994 年 9 月，同样的事件爆发，不过主角换成了阿米巴病毒(Amoeba)。1994 年，俄罗斯黑客弗拉德 • 莱文(Vladimir Levin)侵入了花旗银行(Citibank)的现金管理系统，将 1 亿元纳入自己的账户。1996 年，Boza 病毒出现并感染了号称百毒不侵的 Windows 95 操作系统。1998 年，第一个 Java 病毒 Strange Brew 问世。

进入 21 世纪，2005 年，病毒 Bropia 蠕虫感染了因特网，锁定 MSN Messenger 作为传播源。2007 年，一种名为风暴蠕虫(Storm Worm)的病毒席卷了成千上万的电子邮箱，这种特洛伊木马变种病毒携带一个可执行文件作为附件发给用户，一旦打开附件，计算机便在不知情下变成僵尸网络的一员，传播病毒和恶意广告。

在众多的网络安全事件中，一部分通过网络安全部门的调查取证，已经找出了肇事者并处以相应的处罚，有一些网络犯罪疑案至今悬而未决，各大网络安全部门和公司对此也一筹莫展。PCMAG 选出了史上十大最悬疑的计算机网络犯罪案件，其中就包括前面提到的 WANK 蠕虫。

(1) 1989 年 10 月，WANK 蠕虫入侵 NASA。

某个家伙为了抗议钚驱动的伽利略探测器的发射而入侵了美国宇航局 NASA 系统，造成了 50 万美元的损失。当年受 WANK 病毒攻击后的计算机屏幕如图 2-1 所示。

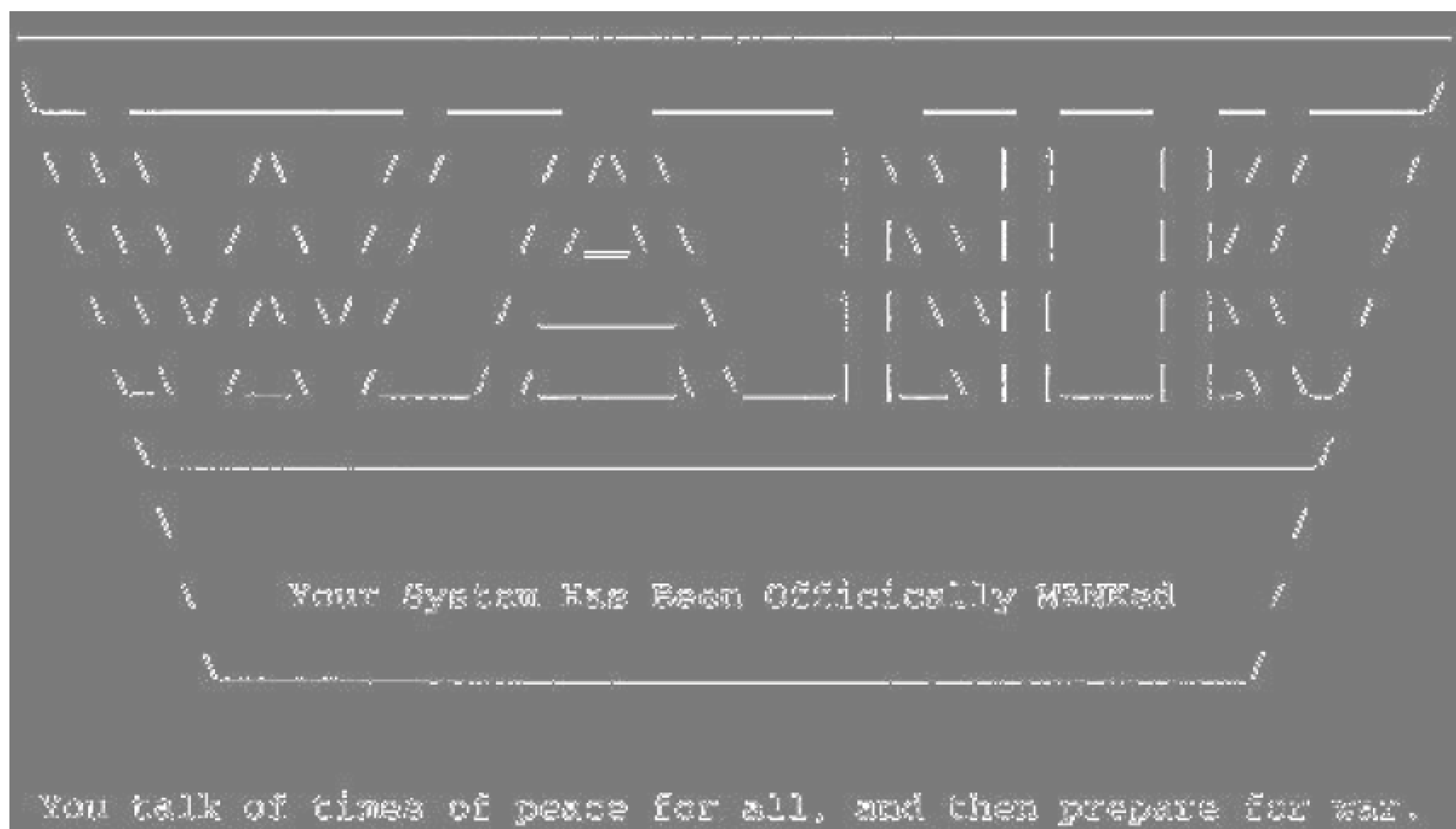


图 2-1　WANK 病毒界面

(2) 1999 年 2 月，美国国防部卫星被黑客入侵。

(3) 2000 年 1 月，信用卡信息失窃。

(4) 2000 年 12 月，军用源代码泄露。

(5) 2001 年 10 月，微软数字版权保护被破解。

(6) 2003 年 10 月，总统竞选主页被黑。

(7) 2006 年 3 月，MBA 录取系统被破解。

(8) 2007 年冬，两万网站被黑。

(9) 2008 年 2 月，超市客户信用卡被盗。

(10) 2008 年 5 月，Comcast 被黑。

一个名叫 Kryogeniks 的黑客组织黑掉了 comcast.net 的域名注册商 Network Solutions(NTSL 是美国一个大型域名服务商，包括微软和 IBM 在内很多大公司域名均由其管理)并篡改了域名 DNS 记录，被黑的 Comcast 网页如图 2-2 所示。

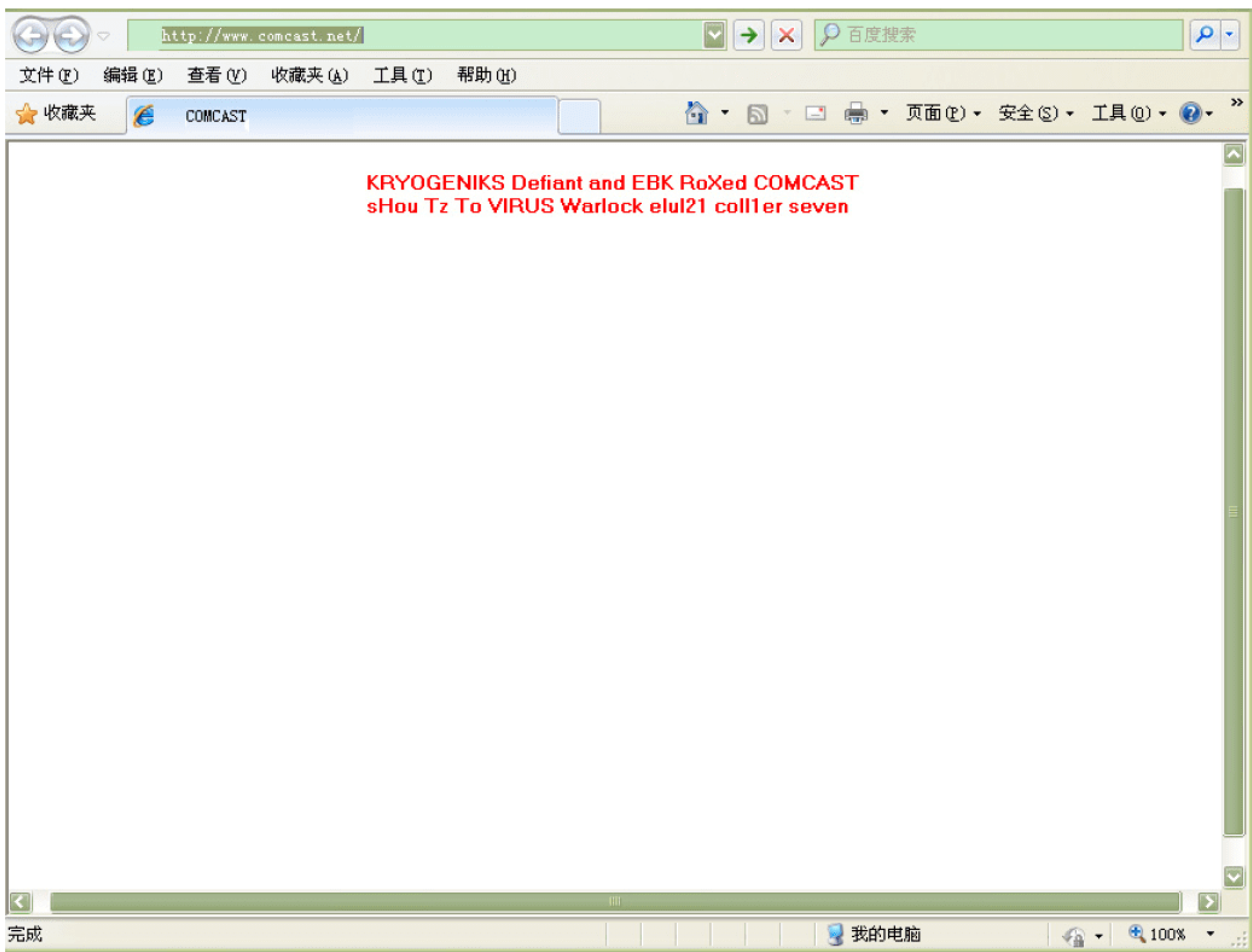


图 2-2　Comcast 被黑的网页

诸如此类的网络犯罪案件，已经屡见不鲜，并且有愈演愈烈之势，因此而带来的日渐升级的网络安全问题也愈发显出它的重要性和急迫性。网络安全的发展，就是如何与这些不断涌现并升级的病毒、新的攻击手段和技术以及非法入侵者进行斗智斗勇的过程。

2. 网络安全发展阶段

纵观网络信息安全的历史，其发展过程经历了三个阶段。

(1) 通信安全阶段

在早期，通信技术还不发达，电脑只是零散地位于不同的地点，信息系统的安全一方面局限于保证电脑的物理安全以及通过密码(主要是序列密码)解决通信安全保密问题。把电脑安置在相对安全的地点，不容许生人接近，就可以保证数据的安全性。但是，信息是必须要交流的。如果这台电脑的数据需要让别人读取，而需要数据的人在异地，怎么办？只有将数据复制在介质上，派专人秘密送到目的地，复制进电脑再读取出数据。即使是这样，也不是完美无缺了，谁来保证信息传递员的安全？因此这个阶段人们强调的信息系统安全性更多的是信息的保密性，对安全理论和技术的研究也仅限于密码学，这一阶段的信息安全可以简单地称为通信安全，它侧重于保证数据在从一地传送到另外一地时的安全。

(2) 信息安全阶段

进入 20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过电脑网络来完成。这时候的信息已经分成了静态信息和动态信息。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能正确读出信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。

1977年美国国家标准局(NBS)公布的国家数据加密标准(DES)和1983年美国国防部公布的《可信计算机系统评价准则》(TCSEC，Trusted Computer System Evaluation Criteria，1985年再版)标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶，后者就是著名的橘皮书。这一时期，国际上把相应的信息安全工作称为数据保护。

(3) 信息保障阶段

到了20世纪90年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性三个原则，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段。换句话说，仅仅保证动态信息是不够的，因为静态信息已经被连接到了互联网上，这个阶段的任务是防止互联网上的不良者破坏静态信息或非法获取静态信息。

2.1.2　网络安全的含义、要素

网络安全涉及的领域相当广泛，这是因为目前的计算机网络中存在各种各样的安全漏洞和威胁。从广义角度来说，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的范畴。

总结来自各个方面对网络安全的阐述，我们认为它大致应该具备以下几个要素。

1. 可靠性

指网络信息能够在规定条件下和指定时间内实现规定功能的特性。可靠性是网络安全的最基本要求之一，是所有网络信息系统建设和运行的目标。

2. 保密性

指信息不泄露给非授权用户、实体或供其利用。通俗一点说，就是防止信息泄露给非授权的个人或实体，信息只提供给授权用户使用。

3. 完整性

指数据未经授权不能进行修改，即数据在传输和存储过程中应该保持不被删除、修改、伪造、乱序、重放、插入、破坏和丢失。完整性是信息的安全性，它要求保持信息的原样，即信息的正确生成、存储和传输。

4. 可用性

指可以被授权实体访问并按需求使用，即当合法授权的群体需要时应该能够存取所需的信息。可用性应该满足身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪等要求。

5. 可控性

指对信息的传播和内容具备控制能力。保障系统根据授权提供服务，使系统在任何时候都不被非授权用户使用。即对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采

取有效防范措施。

6. 不可抵赖性

也称作不可否认性。在网络信息的交互过程中，确认参与者的真实统一性，即所有参与者都不能否认或抵赖曾经进行过的操作和承诺。利用源信息证据防止发信息一方否认已发送信息，同时利用接收的信息证据防止事后接收方否认已经接收信息。

2.2　网络面临的安全威胁

计算机网络的发展，使信息的共享应用日益广泛与深入。但是信息在网络上传输、存储、共享，会被非法窃听、截取、篡改或损坏，因此导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事部门对网络上传输和存储信息的安全问题更为敏感。

对网络信息构成不安全的因素很多，其中包括人为的因素、自然的和偶然发生的因素。人为的安全威胁来自于一些不法之徒利用计算机网络存在的漏洞，或者潜入机房或者终端设备所在场所，通过技术手段盗窃系统资源、非法获取重要数据、篡改系统信息、破坏硬件设备、编写计算机病毒程序并发布传播等。显然，人为因素是对计算机信息网络安全最大的威胁。

2.2.1　非人为安全威胁

非人为因素造成对计算机网络安全的威胁大致有：计算机物理安全、操作系统的安全漏洞、各种自然灾害对计算机构成的威胁以及一些偶发性的因素如电源故障、设备机能失常等对计算机网络构成的严重威胁。随着计算机网络硬件设备的不断改进升级，安全防范措施的不断完善，非人为因素对网络造成的威胁已经被控制在可接受的范围内。

2.2.2　人为安全威胁

人为因素对计算机网络造成的威胁，主要体现在非授权访问网络信息资源，信息泄露，数据篡改和删除，拒绝服务，破坏网络硬件设备，计算机病毒的发布传播等，这些可以归纳为主观意义上的安全威胁。此外还有一些非主观意识上的网络安全威胁，也是由于人为因素造成的，来自于网络管理制度的不健全、安全管理水平的低劣、误操作、渎职行为等，都会对计算机网络信息造成一定的威胁。

在第 3 和第 4 章，我们将着重探讨计算机物理安全与操作系统的安全问题。关于人为因素造成的威胁方面的安全防范问题，我们将在后续章节里详细讨论，在此不做详述。

2.3　网络安全需求分析

根据实际需要的不同，网络安全在不同的环境和应用中有不同的需求。

2.3.1　网络物理安全需求

要保证计算机网络系统的安全、可靠，必须保证系统实体有个安全的物理环境条件。这个安全的环境是指机房及其设施，主要包括以下内容。

(1) 计算机系统的安全环境条件，包括温度、湿度、空气洁净度、腐蚀度、虫害、振动和冲击、电气干扰等方面，都要有具体的要求和严格的标准。

(2) 计算机系统选择一个合适的安装场所十分重要，它直接影响到系统的安全性和可靠性。选择计算机房场地，要注意其外部环境安全性、地质可靠性、场地抗电磁干扰性，避开强振动源和强噪声源，并避免设在建筑物高层和用水设备的下层或隔壁。

(3) 机房的安全防护是针对环境的物理灾害和防止未授权的个人或团体破坏、篡改或盗窃网络设施、重要数据而采取的安全措施和对策。

2.3.2　网络系统安全需求

操作系统是作为一个支撑软件，使得程序或别的应用系统在上面正常运行的一个环境。操作系统提供了很多的管理功能，主要是管理系统的软件资源和硬件资源。操作系统软件自身的不安全性，系统开发设计的不周而留下的破绽，都给网络安全留下隐患。

1. 系统结构的缺陷

操作系统本身有内存管理、CPU 管理、外设的管理，每个管理都涉及一些模块或程序，如果在这些程序里面存在问题，比如内存管理的问题，外部网络的一个连接，刚好连接到一个有缺陷的模块，可能出现的情况是，计算机系统因此而崩溃。

系统支持在网络上传送文件、加载或安装程序，包括可执行文件，这些功能也会带来不安全因素。网络很重要的一个功能就是文件传输功能，如 FTP，这些安装程序经常会带一些可执行文件，这些可执行文件都是人为编写的程序，如果某个地方出现漏洞，那么可能就会造成系统崩溃。像这些远程调用、文件传输，如果生产厂家或个人在上面安装间谍程序，那么用户的整个传输过程、使用过程都会被别人监视到，所有的这些传输文件、加载的程序、安装的程序、执行文件，都可能给操作系统带来安全的隐患。

2. 进程的安全

系统不安全的一个原因在于它可以创建进程，支持进程的远程创建和激活，支持被创建的进程继承创建的权利，这些机制提供了在远端服务器上安装“间谍软件”的条件。

守护进程是系统的一些进程，总是在等待某些事件的出现。所谓守护进程，比如说用户有没有按键盘或鼠标，或者别的一些处理。一些监控病毒的监控软件也是守护进程，这些进程可能是好的，比如防病毒程序，一有病毒出现就会捕捉到。如果操作系统中有些守护进程被人破坏掉就会出现不安全的情况。

3. 远程调用

系统会提供一些远程调用功能，所谓远程调用就是一台计算机可以调用远程计算机或大型服务器里面的一些程序，可以提交程序给远程的服务器执行，如 telnet。远程调用要经过很

多环节，中间的通信环节可能会出现被人监控等问题。

4. 系统后门和漏洞

后门程序是指那些绕过安全控制而获取对程序或系统访问权的程序方法。在软件开发阶段，程序员利用软件的后门程序得以便利地修改程序设计中的不足。一旦后门被黑客利用，或在发布软件前没有删除后门程序，容易被黑客当成漏洞进行攻击，造成信息泄密和丢失。

尽管系统的漏洞可以通过版本的不断升级来克服，但是系统的某一个安全漏洞就会使得系统的所有安全控制毫无价值。从发现问题到升级这段时间，一个小小的漏洞就足以使整个网络瘫痪掉。

2.3.3　网络应用安全需求

网络安全在不同的环境和应用中，有不同的需求。

从用户(个人、企业等)的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免他人或竞争对手用窃听、假冒、篡改等手段对用户的合法权益和隐私造成侵犯。

从网络运营和管理者的角度来说，他们希望对网络信息的访问、读写等操作受到保护和控制，避免出现病毒传播、非法存取、拒绝服务和网络资源非法占用和控制等问题，并且具备一定的制止和防御网络黑客攻击的能力。

对于安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和屏蔽，避免这些信息通过网络泄露，防止由于这类信息的泄露对社会造成的危害，对国家造成的损失，甚至对国家安全造成威胁。

从社会教育和意识形态的角度来说，网络上不健康的内容会对社会的安定团结和青少年的健康成长带来负面的影响，必须加以监督和控制。

2.3.4　网络数据安全需求

网络数据安全突出表现在数据的保密性、完整性和可用性方面。

具体到以数据库为例，数据库管理系统的大量信息存储在各种各样的数据库里面，包括我们上网看到的所有信息，数据库主要考虑的是方便存储、利用和管理信息，但在安全方面考虑得比较少。例如：授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核，窃取信息。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性。数据的安全性是防止数据库被破坏和非法的存取；数据库的完整性是防止数据库中存在不符合语义的数据。可用性体现在合法授权用户需要访问的数据信息，应该保证任何时候都可以被访问和存取。

2.3.5　网络安全管理

计算机网络的安全管理，不仅要看所采用的安全技术和防范措施，而且要看它所采取的管理措施和执行计算机安全保护法律、法规的力度。只有将两者紧密结合，才能使计算机网络安全确实有效。

计算机网络的安全管理，包括对计算机用户的安全教育、建立相应的安全管理机构、不断完善和加强计算机的管理功能、加强计算机及网络的立法和执法力度等方面。加强计算机安全管理，加强用户的法律、法规和道德观念，提高计算机用户的安全意识，对防止计算机犯罪、抵制黑客攻击和防止计算机病毒干扰，是十分重要的措施。

2.4　网络安全模型和体系结构

2.4.1　安全模型

网络安全模型是动态网络安全过程的抽象描述。通过对安全模型的研究，了解安全动态过程的构成因素，是构建合理并实用的安全策略体系的前提之一。为了达到安全防范的目的，需要建立合理的网络安全模型，以指导网络安全工作的部署和管理。目前，在网络安全领域存在较多的网络安全模型，在此介绍两种常见的模型：PDRR 模型和 PPDR 模型。

1. PDRR 安全模型

PDRR 即美国国防部提出的常见的“信息安全保障体系”，它概括了网络安全的整个环节，包括防护(Protection)、检测(Detection)、响应(Response)、恢复(Recovery)。PDRR 模型的名称也由这 4 个环节的英文单词首字母组合而来，这 4 个部分构成了一个动态的信息安全周期，如图 2-3 所示。

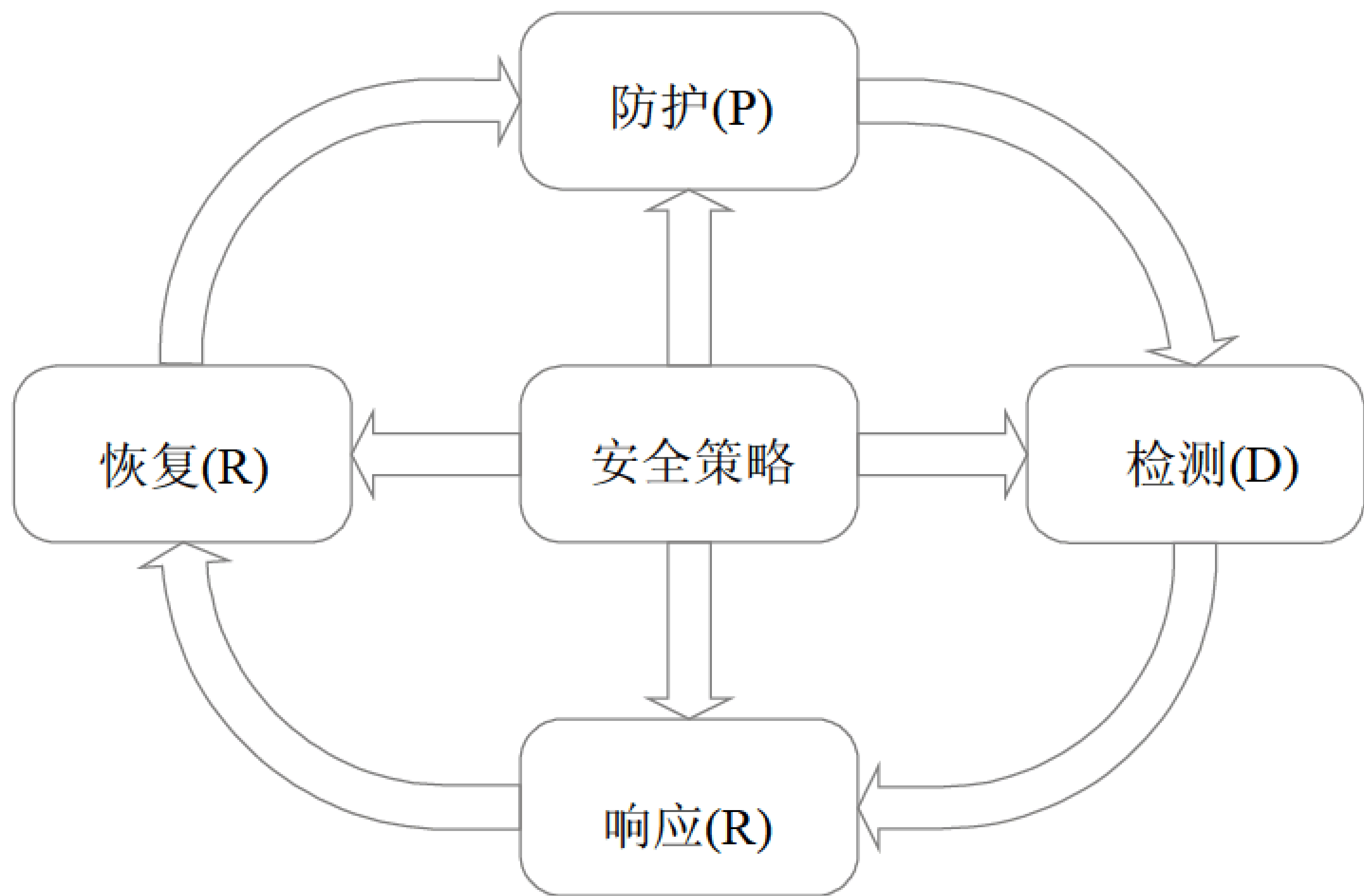


图 2-3　PDRR 安全模型

PDRR 安全模式提出了人、政策(包括法律、法规、制度、管理)和技术三大要素；归纳了网络安全的主要内涵，即鉴别、保密、完整性、可用性、不可抵赖性、责任可核查性和可恢复性；提出了信息安全的几个重点领域，即关键基础设施的网络安全(包括电信、油气管网、交通、供水、金融等)、内容的信息安全(包括反病毒、电子信箱安全和有害内容过滤等)和电子商务的信息安全；认为密码理论和技术是核心，安全协议是桥梁，安全体系结构是基础，安全的芯片是关键，监控管理是保障，攻击和评测的理论和实践是考验。

1) 防护

防护是 PDRR 模型的最重要部分。防护是预先阻止攻击可能发生的条件产生，让攻击者无法顺利入侵。防护可以抵御大多数的入侵事件，它包括缺陷扫描、访问控制、防火墙、数据加密及鉴别等。

(1) 缺陷扫描

安全缺陷分为两种：允许远程攻击的缺陷和只允许本地攻击的缺陷。允许远程攻击的缺陷就是攻击者可以利用该缺陷，通过网络攻击系统。只允许本地攻击的缺陷就是攻击者不能通过网络利用该缺陷攻击系统。对于允许远程攻击的安全缺陷，可以用网络缺陷扫描工具去发现。网络缺陷扫描工具一般从系统的外边去观察。其次，它扮演一个黑客的角色，只不过它不会破坏系统。缺陷扫描工具首先扫描系统所开放的网络服务端口，然后通过该端口进行连接，试探提供服务的软件类型和版本号。在这个时候，缺陷扫描工具有两种方法去判断该端口是否有缺陷：第一种方法是根据版本号，在缺陷列表中查出是否存在缺陷。第二种方法是根据已知的缺陷特征，模拟一次攻击。如果攻击表示可能会成功，就停止并认为是缺陷存在(要停止攻击模拟避免对系统损害)。显然第二种方法的准确性比第一种要好，但是它扫描的速度会很慢。

(2) 访问控制与防火墙

访问控制限制某些用户对某些资源的操作。访问控制通过减少用户对资源的访问，从而减少资源被攻击的概率，达到防护系统的目的。例如只让可信的用户访问资源而不让其他用户访问资源，这样资源受到攻击的概率几乎很小。防火墙是基于网络的访问控制技术，在 Internet/Intranet 中的广泛应用已经成为不争的事实。防火墙技术可以工作在网络层、传输层和应用层，完成不同粒度的访问控制。防火墙可以阻止大多数的攻击但不是全部，很多入侵事件通过防火墙所允许的规则进行攻击，例如通过 80 端口进行攻击。

(3) 病毒防治

病毒就是计算机的一段可执行代码，这些病毒感染到计算机上的过程完全是被动的。计算机病毒的传统感染过程并不是利用系统上的缺陷。只要用户直接跟这些病毒接触，例如复制文件、访问网站、接受 E-mail 等，该用户的系统就会被感染。一旦计算机被感染上病毒，这些可执行代码可以自动执行，破坏计算机系统。安装并经常更新防病毒软件会对系统安全起防护作用。防病毒软件根据病毒的特征，检查用户系统上是否有病毒。这个检查过程可以是定期检查，也可以是实时检查。

(4) 数据加密

加密技术保护数据在存储和传输中的保密性安全。所谓加密，就是数据经过一种特殊处理使其看起来毫无意义，同时仍保持可以对其恢复成原始数据的途径。这个特殊处理的过程称为加密。加密之前的原始数据被称为明文。加密之后的数据被称为密文，从密文恢复到明文的过程叫解密。

一般来说，加密和解密的算法通常都是公开的。唯一使得数据得到保护的因素就是密钥。密钥其实是一个数值，加密算法使用这个数值对明文进行编码。解密算法就是用与之对应的密钥进行解码。

加密有两种：对称加密技术和公开密钥加密技术。在对称加密技术中，加密和解密过程使用同一密钥。数据加密标准(Data Encryption Standard，DES)就是对称加密方法的一个实例。在公开密钥加密技术中，加密和解密过程使用一对非对称的密钥：公开密钥和私有密钥。公开密钥可以让所有人知道，私有密钥则要保密。从公钥推导出密钥需要超大的计算量，实际上是不可行的。

(5) 鉴别技术

鉴别技术和数据加密技术有很紧密的关系。鉴别技术用在安全通信中，对通信双方互相鉴别对方的身份以及传输的数据。鉴别技术保护数据通信的两个方面：通信双方的身份认证和传输数据的完整性。鉴别技术主要使用公开密钥加密算法的鉴别过程，即如果个人用自己的私有密钥对数据加密为密文，那么任何人都可以用相应的公开密钥对密文解密，但不能创建这样的密文，因为没有相应的私有密钥。

数字签名是在电子文件上签名的技术，确保电子文件的完整性。数字签名首先使用消息摘要函数计算文件内容的摘要，再用签名者的私有密钥对摘要加密。

身份认证需要每个实体(用户)登记一个数字证书。这个数字证书包含该实体的信息(如用户名、公开密钥)。另外，这个证书应该有一个权威的第三方签名，保证该证书上的内容是有效的。

2) 检测

PDRR 模型的第二个环节就是检测(D)。上面提到防护系统除掉入侵事件发生的条件，可以阻止大多数的入侵事件的发生，但是它不能阻止所有的入侵。特别是那些利用新的系统缺陷、新的攻击手段的入侵。因此安全策略的第二个安全屏障就是检测，即如果入侵发生就检测出来，这个工具是入侵检测系统(Intrusion Detection System，IDS)。通常采用入侵检测系统(IDS)来检测系统漏洞和缺陷，增加系统的安全性能，从而消除攻击和入侵的条件。

检测并不是根据网络和系统的缺陷，而是根据入侵事件的特征去检测的。但是，黑客攻击系统的时候往往是利用网络和系统的缺陷进行的，所以入侵事件的特征一般与系统缺陷的特征有关系。因此防护和检测技术是有相关的理论背景的。

入侵检测系统(IDS)是一个硬件系统和软件程序，它的功能是检测出正在发生或已经发生的入侵事件。这些入侵已经成功地穿过防护战线。一个入侵检测系统有很多特征，其主要特征为：检测环境和检测算法。根据不同的特征，入侵检测系统可以分为不同的类型。

根据检测环境不同，IDS 一般可以分为基于主机的 IDS(Host-based)和基于网络的IDS(Network-based)。基于主机的 IDS 检测基于主机上的系统日志、审计数据等信息，而基于网络的 IDS 检测则一般侧重于网络流量分析。

根据检测所使用的方法，IDS 还可以分为两种：误用检测(Misuse Detection)和异常检测(Anomaly Detection)。误用检测技术需要建立一个入侵规则库，其中，它对每一种入侵都形成一个规则描述，只要发生的事件符合于某个规则就被认为是入侵。

入侵检测系统一般和紧急响应及系统恢复有密切关系。一旦入侵检测系统检测到入侵事件，它就会将入侵事件的信息传给应急响应系统进行处理。

3) 响应

PDRR 模型中的第三个环节就是响应(R)。响应就是已知一个攻击(入侵)事件发生之后进行处理。在一个大规模的网络中，响应这个工作都由一个特殊部门负责，那就是计算机响应小组。世界上第一个计算机响应小组 CERT，位于美国 CMU 大学的软件研究所(SEI)，于 1989 年建立，是世界上最著名的计算机响应小组。从 CERT 建立之后，世界各国以及各机构也纷纷建立自己的计算机响应小组。我国第一个计算机紧急响应小组 CCERT，于 1999 年建立，主要服务于中国教育和科研网。

入侵事件的报警可以是入侵检测系统的报警，也可以是通过其他方式的汇报。响应的主要工作也可以分为两种：第一种是紧急响应；第二种是其他事件处理。紧急响应就是当安全事件发生时采取应对措施，其他事件主要包括咨询、培训和技术支持。

4) 恢复

恢复是 PDRR 模型中的最后一个环节。恢复是事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。恢复也可以分为两个方面：系统恢复和信息恢复。系统恢复指的是修补该事件所利用的系统缺陷，不让黑客再次利用这样的缺陷入侵。一般系统恢复包括系统升级、软件升级和打补丁等。系统恢复的另一个重要工作是除去后门。一般来说，黑客在第一次入侵的时候都是利用系统的缺陷。在第一次入侵成功之后，黑客就在系统打开一些后门，如安装一个特洛伊木马。

所以，尽管系统缺陷已经打补丁，黑客下一次还可以通过后门进入系统。系统恢复都是根据检测和响应环节提供有关事件的资料进行的。信息恢复指的是恢复丢失的数据。数据丢失可能是由于黑客入侵造成的，也可以是由于系统故障、自然灾害等原因造成的。信息恢复就是从备份和归档的数据恢复原来数据。信息恢复过程跟数据备份过程有很大的关系。数据备份做得是否充分对信息恢复有很大的影响。信息恢复过程的一个特点是有优先级别。直接影响日常生活和工作的信息必须先恢复，这样可以提高信息恢复的效率。

在上述的安全的 4 个环节基础上，PDRR 模型引进了时间的概念。

(1) 保护时间(Pt)

表示从入侵开始到成功侵入系统的时间，即攻击所需时间。高水平的入侵及安全薄弱的系统都能导致攻击的有效性，使保护时间 Pt 缩短。

(2) 检测时间(Dt)

系统安全检测包括发现系统的安全隐患和潜在攻击检测。改进检测算法和设计可缩短 Dt，适当的防护措施可有效缩短 Dt。

(3) 响应时间(Rt)

包括检测到系统漏洞或监控到非法攻击到系统启动处理措施的时间。例如一个监控系统的响应可能包括监视、切换、跟踪、报警、反攻等内容。而安全事件的后处理(如恢复、事后总结等)不纳入事件响应的范畴之内。

PDRR 模型用数学公式的方法简明地解析了安全的概念：系统的保护时间应大于系统检测到入侵行为的时间加上系统响应时间，即 $Pt > Dt+Rt$。也就是在入侵者危害安全目标之前就能够被检测到并被及时处理。巩固的防护系统与快速的反应结合起来，就是真正的安全。例

如，防盗门只能延长被攻破的时间。如果警卫人员能够在防盗系统被攻破之前作出迅速反应，那么这个系统就是安全的。这实际上给出了安全的一个全新的定义：及时的检测和响应就是安全。根据这样一种安全理论体系，我们就知道构筑网络安全的宗旨就是提高系统的防护时间，降低检测时间和响应时间。

(4) 系统暴露时间(Et)

指系统处于不安全状况的时间，等于检测到入侵者破坏安全目标开始，将系统恢复到正常状态的时间。系统的暴露时间越长，系统就越不安全。例如，对 Web 服务器被破坏的页面进行恢复。

PDRR 阐述了这样一种理念：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间，在系统遭到破坏后，尽快恢复正常工作，以减少系统暴露时间。

当然，PDRR 模型表现为网络安全最终的存在形态，是一类目标体系和模型，它并不关注网络安全建设的工程过程，并没有阐述实现目标体系的途径和方法。此外，模型更侧重于技术，对诸如管理这样的因素并没有强调。网络安全体系应该是融合了技术和管理在内的一个可以全面解决安全问题的体系结构，它应该具有动态性、过程性、全面性、层次性和平衡性等特点，是一个可以在信息安全实践活动中真正依据的建设蓝图。

2. PPDR 安全模型

PPDR(Policy Protection Detection Response)模型是美国 ISS(Internet Security Systems)公司提出的动态网络安全体系的代表模型，也是动态安全模型的雏形。PPDR 模型包括四个主要部分：安全策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)，如图 2-4 所示。

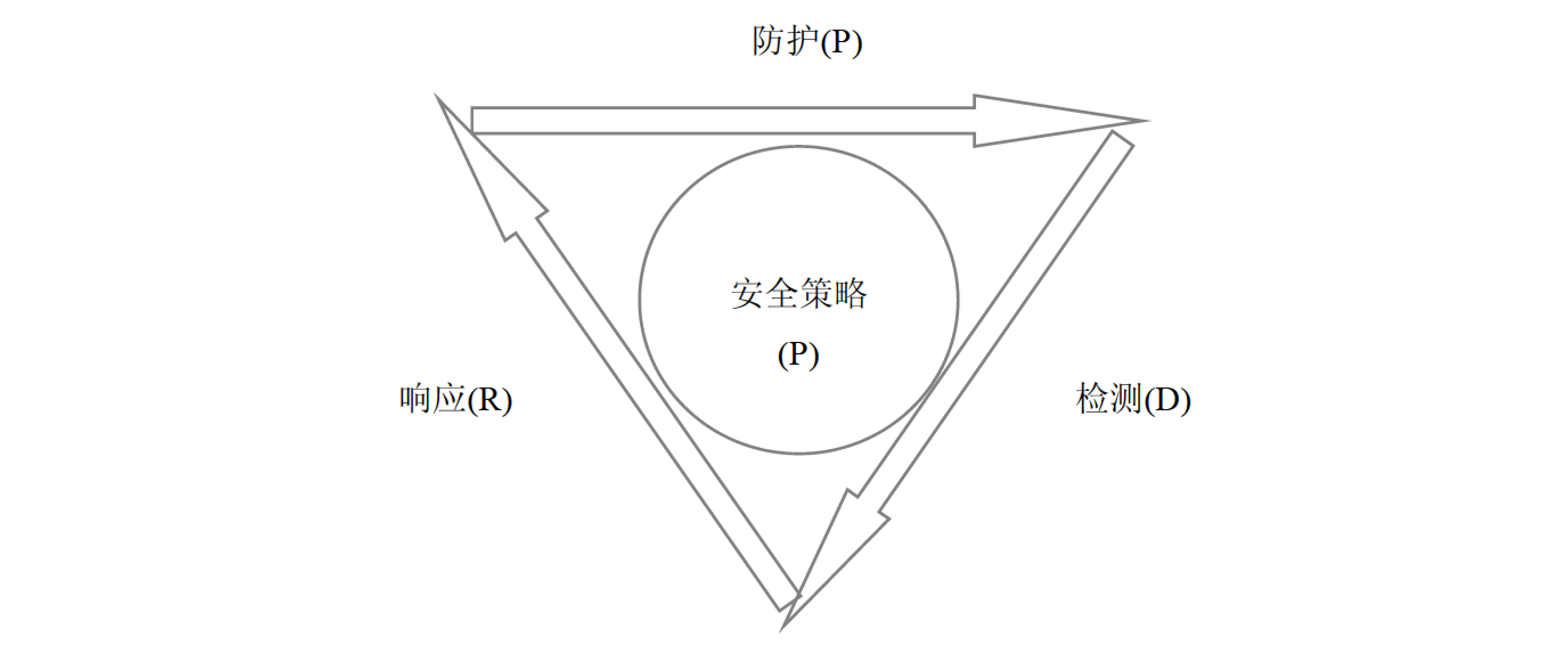


图 2-4　PPDR 安全模型

PPDR 的基本思想是：以安全策略为核心，通过一致性检查、流量统计、异常分析、模式匹配以及基于应用、目标、主机、网络的入侵检查等方法进行安全漏洞检测。检测使系统从静态防护转化为动态防护，为系统快速响应提供了依据。当发现系统有异常时，根据系统安全策略快速做出反应，从而达到保护系统安全的目的。

(1) 安全策略

PPDR 安全模型的核心是安全策略。所有的防护、检测、响应都是安全策略实施的。安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制定、评估、执行等。策略是这个模型的核心，意味着网络安全要达到的目标，它决定各种措施的强度。

(2) 防护

防护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可抵赖性。防护应该依据不同等级的系统安全要求来完善系统的安全功能和安全机制。防护通常采用身份认证、防火墙、客户端软件、加密等传统的安全技术来实现。

防护是安全的第一步，包括：制定安全规章(以安全策略为基础制定安全细则)，配置系统安全(配置操作系统、安装补丁等)，采用安全措施(安装使用防火墙、VPN 等)。

(3) 检测

检测是对上述二者的补充，通过检测发现系统或网络的异常情况，发现可能的攻击行为。检测是 PPDR 模型中非常重要的环节，是进行动态响应和动态保护的依据，同时强制网络按照安全策略，检测设备不间断地检测、监控网络和系统，及时发现网络中的威胁和存在的弱点，通过循环的反馈及时做出响应。网络的安全风险是无时不在的。检测的对象主要针对系统自身的脆弱性和外部威胁。

(4) 响应

响应是指在系统检测到安全漏洞后做出的处理方法，它在 PPDR 安全模型中占重要地位，是解决潜在的安全问题最有效的方法。

响应是在发现异常或攻击行为后系统自动采取的行动，目前的入侵响应方式也比较单一，主要就是关闭端口、中断连接、中断服务等方式。研究多种入侵响应方式将是今后的发展方向之一。

PPDR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具(如防火墙、操作系统身份认证、加密等)的同时，利用检测工具(如漏洞评估、入侵检测等)了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

该理论的最基本原理认为信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为还是响应行为等都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。当然攻击成功花费的时间就是安全体系提供的防护时间(Pt)；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间，即检测时间(Dt)；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间，即响应时间(Rt)。

PPDR 模型可以用一些典型的数学公式来表达安全的要求：

公式 1：Pt > Dt + Rt。

Pt 代表系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客(入侵者)攻击安全目标所花费的时间。Dt 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。Rt 代表从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。那么，针对需要保护的安全目标，如果上述数学公式满足防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能被检测到并及时处理。

公式 2：Et = Dt + Rt，如果 Pt = 0。

公式的前提是假设防护时间为 0。Dt 代表从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。Rt 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对 Web Server 被破坏的页面进行恢复。那么，Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对需要保护的安全目标，Et 越小系统就越安全。

通过对上面两个公式的描述，实际上给安全下了一个全新的定义："及时的检测和响应就是安全"、"及时的检测和恢复就是安全"。

而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间(Pt)，降低检测时间(Dt)和响应时间(Rt)。

PPDR 模型也存在一个明显的弱点，就是忽略了内在的变化因素，如人员的流动、人员的素质和策略贯彻的不稳定性。实际上，安全问题牵涉面广，除了涉及防护、检测和响应，系统本身安全的"免疫力"的增强、系统和整个网络的优化，以及人员这个在系统中最重要角色的素质的提升，都是该安全系统没有考虑到的问题。

2.4.2　安全体系结构

所谓安全体系结构，指的是一个计划和一套原则，它应该描述：

- 为满足用户需求而必须提供的一套安全服务；
- 要求所有系统元素都要实现的服务；
- 为应付威胁环境而要求系统元素达到的安全级别。

一个安全体系结构是采用系统工程过程的结果，一个完整的安全体系结构包括管理安全、通信安全、计算机安全、辐射安全、人员安全和物理安全等。它既要应付恶意威胁，也要应付意外的威胁。与 OSI 参考模型对应的网络信息安全体系结构三维模型如图 2-5 所示。其中 *X* 轴表示安全机制，*Y* 轴表示 OSI 参考模型，*Z* 轴表示安全服务。

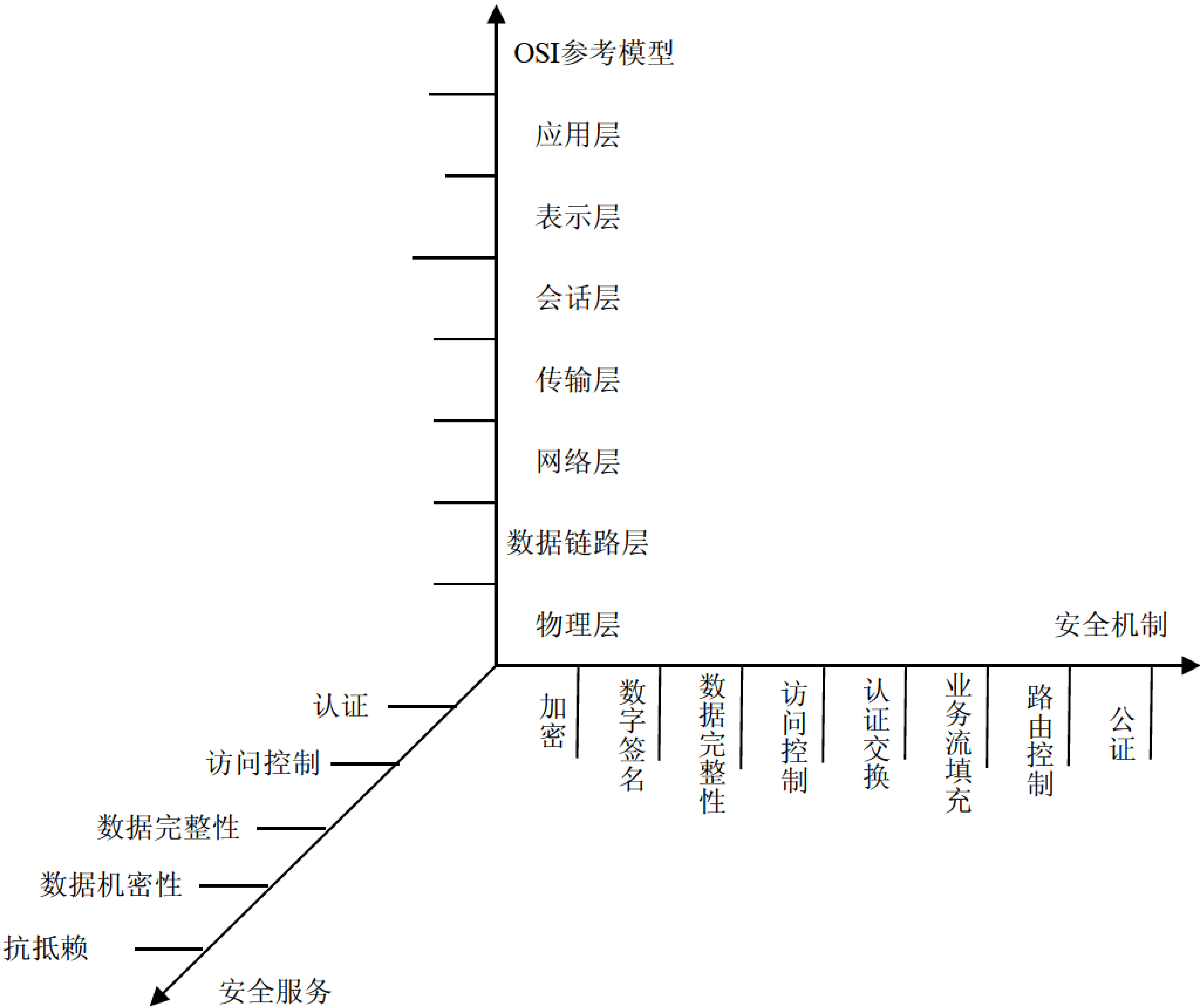


图 2-5　OSI 网络安全体系结构三维模型

与安全体系结构相关的概念还有安全机制、安全模型、安全服务和安全策略等。

(1) 安全机制：安全机制是一个过程(或与该过程绑定的一种设备)。它能用于一个系统，使该系统能够实现对外或对内提供的安全服务。安全机制的实例有鉴别交换、校验和数字签名、加密、传输填充等。

(2) 安全模型：它描述了一个系统对外或对内提供的一套规定的安全服务。

(3) 安全策略：安全策略指一套规则和惯例，它详细说明了系统或者组织如何提供安全服务去保护敏感的关键系统资源。例如：基于身份的安全策略、基于规则的安全策略等。

(4) 安全服务：指系统提供的一种处理服务或通信服务。它能够为系统资源提供特定的保护，如访问控制服务、审计服务、有效性服务、数据加密性服务、数据完整性服务、数据源认证服务、不可抵赖性服务、对等实体认证服务、系统完整性服务等。安全服务实现了安全策略，并且由安全机制实现。

信息安全保障体系的建设策略是要建立信息安全防护能力，要具有隐患发现能力、网络反应能力、信息对抗能力。在建立我国的信息安全保障体系时，有人主张在 PDRR 的前面加上预警，在后面加上反击。

预警的基本宗旨就是根据以前掌握的系统脆弱性，了解当前的犯罪趋势，预测未来可能受到的攻击和危害。作为预警，首先要分析威胁来源与方式，分析系统的脆弱性，评估资产与风险，考虑使用什么强度的保护可以消除、避免、转嫁风险，剩下的风险能否承受。

反击就是利用高技术工具，提供犯罪分子犯罪的线索、依据，依法侦查犯罪分子，处理犯罪案件，要求形成取证能力和打击手段，依法打击犯罪和网络恐怖主义分子。

计算机网络安全技术主要有实时扫描技术、实时监测技术、防火墙技术、完整性检验保

护技术、病毒情况分析报告技术和系统安全管理技术。综合起来，可以采取以下方式。

1. 建立安全管理制度

提高包括系统管理员和用户在内的人员的技术素质和职业道德修养。对重要部门和信息，严格做好开机查毒，及时备份数据，这是一种简单有效的方法。

2. 网络访问控制

访问控制是网络安全防范和保护的主要策略。它的主要任务是保证网络资源不被非法使用和访问，它是保证网络安全最重要的核心策略之一。

3. 数据库的备份与恢复

数据库的备份与恢复是数据库管理员维护数据安全性和完整性的重要操作。备份是恢复数据库最容易和最能防止意外的保证方法。恢复是在意外发生后利用备份来恢复数据的操作。有三种主要备份策略：只备份数据库、备份数据库和事务日志、增量备份。

4. 应用密码技术

应用密码技术是信息安全核心技术，密码手段为信息安全提供了可靠保证。基于密码的数字签名和身份认证是当前保证信息完整性的最主要方法之一，密码技术主要包括古典密码体制、单钥密码体制、公钥密码体制、数字签名以及密钥管理，详见后续章节。

5. 切断传播途径

对被感染的硬盘和计算机进行彻底杀毒处理，不使用来历不明的 U 盘和程序，不随意下载网络可疑信息。

6. 提高网络反病毒技术能力

通过安装病毒防火墙，进行实时过滤，对网络服务器中的文件进行频繁扫描和监测，在工作站上采用防病毒卡，加强网络目录和文件访问权限的设置。在网络中，限制只能由服务器允许执行的文件。

7. 研发并完善高安全的操作系统

研发具有高安全的操作系统，不给病毒得以滋生的温床才能更安全。

综合安全保障体系可以由实时防御、常规评估和基础设施三部分组成。实时防御系统由入侵检测、应急响应、灾难恢复和防守反击等功能模块构成，入侵检测模块对通过防火墙的数据流进行进一步检查，以阻止恶意的攻击行为，应急响应模块对攻击事件进行应急处理，灾难恢复模块按照策略对遭受破坏的信息进行恢复，防守反击模块按照策略实施反击。常规评估系统利用脆弱性数据库检测与分析网络系统本身存在的安全隐患，为实时防御系统提供策略调整依据。基础设施由攻击特征库、隐患数据库以及威胁评估数据库等基础数据库组成，支撑实时防御系统和常规评估系统的工作。

计算机网络安全是一项复杂的系统工程，涉及技术、设备、管理和制度等多方面的因素，安全解决方案的制定需要从整体上把握。网络安全解决方案是综合各种计算机网络信息系统安全技术，将安全操作系统技术、防火墙技术、病毒防护技术、入侵检测技术、安全扫描技术等综合起来，形成一套完整的、协调一致的网络安全防护体系。我们必须做到管理和技术

并重，安全技术必须结合安全措施，并加强计算机立法和执法的力度，建立备份和恢复机制，制定相应的安全标准。此外，由于计算机病毒、计算机犯罪等技术是不分国界的，因此必须进行充分的国际合作，共同对付日益猖獗的计算机犯罪和计算机病毒等问题。

2.4.3　安全评估标准

安全标准是安全理论和技术用于实践的纲领性规范，是安全理论和技术的总结，对安全产业发展具有指导性作用。安全标准对安全产品的功能、结构及互操作性都提出了要求。安全标准的制定也是一个国家科研水平、技术能力的体现，反映了一个国家的综合实力。安全标准还是加入 WTO 的国家保护自己利益的重要手段，因此，各国都很注重安全标准的研究、制定和推广工作。

回顾一下安全标准发展的过程：第一个有关信息技术安全评价的标准诞生于 20 世纪 80 年代的美国，即著名的《可信计算机系统评价准则》(TCSEC)，俗称橘皮书，它是第一个正式的计算机信息安全评估标准，具有划时代的意义，于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 将安全分为 4 个方面：安全策略、可说明性、安全保障和文档。该标准将计算机系统的安全划分为 4 个类别 8 个级别，按照安全程度由低到高依次是：D1、C1、C2、B1、B2、B3、A1 及超 A1 级。

从 20 世纪 90 年代开始，一些国家和国际组织相继提出了新的安全评价准则。1991 年，欧共体发布了《信息技术安全评价准则》(ITSEC)。1993 年，加拿大发布了《加拿大可信计算机产品评价准则》(CTCPEC)，CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了《信息技术安全评价联邦准则》(FC)。1993 年 6 月，来自六国七方的组织，包括加拿大、法国、德国、荷兰、英国、美国，共同起草了一份通用准则(CC)，并将 CC 推广为国际标准。CC 发布的目的是建立一个各国都能接受的通用的安全评价准则，国家与国家之间可以通过签订互认协议来决定相互接受的认可级别，这样能使基础性安全产品在通过 CC 准则评价并得到许可进入国际市场时，不需要再作评价。

上述各种标准之间存在着一定的相互关系，如图 2-6 所示。

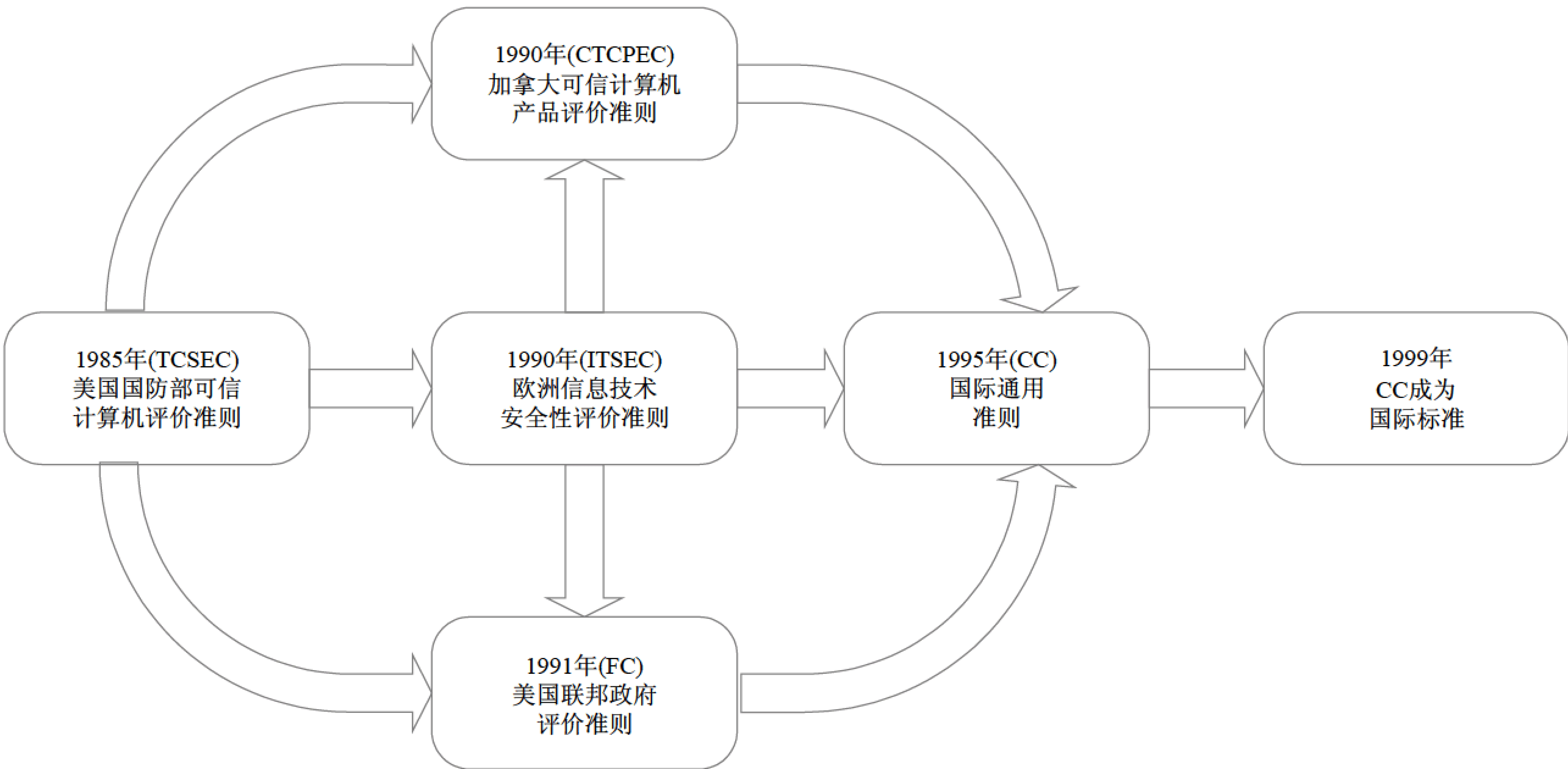


图 2-6　国际安全评测标准及其联系

计算机系统安全评价标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法、执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评价事关国家的安全利益，因此许多国家都在充分借鉴国际标准的前提下，积极制定本国的计算机安全评价认证标准。

本 章 小 结

本章主要介绍了网络安全的基本知识，包括：网络安全发展历程，网络安全的含义和要素；从网络安全面临的威胁、需求分析出发，阐述了安全模型和体系结构，重点介绍了 PDRR 安全模型和 PPDR 安全模型；讲述了国际计算机系统安全评估标准，包括著名的橘皮书 TCSEC、ITSEC、CTCPEC、FC、国际通用准则 CC 以及各种安全标准之间的联系。希望读者通过对本章的学习能够掌握基础的网络安全知识。有关上述安全标准的细节内容，以及中国的信息系统安全标准，我们将在第 15 章中介绍，在此不做赘述，需要了解相关细节的读者请参阅该相关章节。

课 后 练 习

一、 填空题

1. 网络安全发展过程经历了三个阶段，它们是(　　　　)、(　　　　)、(　　　　)。
2. 网络安全的要素，包括(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)。
3. 本文介绍了两种常见的网络安全模型，是(　　　　)、(　　　　)。
4. PDRR 安全模型中的 P、D、R、R 分别代表(　　　　)、(　　　　)、(　　　　)、(　　　　)。
5. 在 TCSEC 标准中，安全级别由高到低分别是(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)、(　　　　)。

二、 选择题

1. TCSEC(Trusted Computer System Evaluation Criteria)俗称(　　)。
   A. 蓝皮书　B. 橘皮书　C. 黄皮书　D. 红宝书
2. TCSEC 标准将计算机系统的安全划分为(　　)个类别，(　　)个级别。
   A. 4　B. 5　C.6　D. 8
3. 下述选项中，(　　)是综合了 TCSEC 和 ITSEC 的优点而制定的安全标准。
   A. FC　B. CC　C. CTCPEC　D. IPSec

4. 下述安全标准中，(　　)是目前的国际通用安全标准。

A. FC　　B. CC　　C. ITSEC　　D. TCSEC

5. 下列要素中，属于网络安全范畴的有(　　)。

A. 完整性　　B. 可移植性　　C. 可靠性　　D. 不可抵赖性

三、 简答题

1. 网络安全的目标主要体现在哪几个方面?
2. 简述 PDRR 安全模型的主要内容。
3. 简述 PPDR 安全模型的主要内容。
4. 简述 TCSEC 安全标准的主要内容。
5. 简述 TCSEC、ITSEC、CTCPEC、FC、CC 安全标准之间的相互关系。

第3章　计算机物理安全

计算机物理安全就是为了保证计算机系统安全可靠性，确保计算机系统在对信息进行采集、处理、传输、存储过程中，不受到人为(包括未授权使用计算机资源)或自然因素的危害，而导致信息丢失、泄露或者破坏，对计算机环境、设备、人员、设施(包括机房建筑、供电、空调等)采取适当的安全防范措施。

本章主要介绍环境的基本安全；机房的安全等级和技术要求；访问控制；磁场、静电防范；电磁波辐射与干扰；电源保护；磁介质的存储与处理；应急备份措施等内容。

本章重点

- 环境安全
- 机房安全及等级
- 设备安全
- 突发应急计划

3.1　环 境 安 全

计算机辅助环境系统的安全统称为计算机环境安全，主要包括计算机设备的位置(在网络环境里，具体体现为计算机机房)、自然灾害的防备、物理选址与建筑材料等。基本的环境安全可以提供计算机系统安全的可靠运行环境。

3.1.1　计算机设备的位置

计算机设备从某种意义上来说属于精密仪器，应该安放在专用的计算机机房或者专门为计算机建造的建筑里，远离街道，远离火源、容易着火的地方或易受潮甚至被水淹没的地方。设备的安放位置不宜利用建筑物外层的房间，也不应该设在锅炉房附近或者有潜在危险的区域，同时要避免放在有高压、大型变压器或发电机等强电辐射源附近。

3.1.2　自然灾害的防备

环境安全措施得当，可以减少发生因火灾、温度和湿度对计算机设备造成的有害影响。将密集的磁盘存储设备分开放置以减少密度，将关键性的存储设备或其他媒介存放在耐火的房间或保险箱内。同时，在防火的房间或保险箱内保存重要的资料文件的副本也非常重要。

在计算机设备密集的环境内应该安放防火器材与设备。为了确保灾害发生时人员能安全撤离及转移设备，应留有必要的空间和通道。环境温度对计算机可靠运行的影响非常明显。有关统计数据表明：对集成电路和电子元器件，室温在规定使用范围内每增加 10℃，其可靠性将降低 25%，期间周围的环境温度超过 60℃，计算机就容易发生故障。温度对电容的影响主要是使其使用寿命缩短，其次是引起电容量和功率等参数的变化。温度对磁介质导磁率的变化也有影响。温度过低会使绝缘材料变硬、变脆。为了克服湿度给计算机设备带来的危害，通常要求把湿度控制在 45%～65%之间。

3.1.3　选址与建筑材料

为了防止计算机设备遭到周围不利环境的意外损害，应尽量避免计算机环境建立在易燃易爆的厂房。另外，应该避开污染区，如化工工业污染区、风沙区、煤场以及有害气体区域等。为了防止爆炸等危险，在与邻室相连接处，最好设置一个缓冲地带或者隔离设施，确保把好第一道关以将火苗遏制住。

3.2　机房安全及等级

中华人民共和国电子工业部 1988 年 4 月 26 日批准，并于 1988 年 10 月 1 日实施了计算机站场地安全要求的国家标准 GB9361—1988，对计算机机房的安全进行了分类。

3.2.1　适用范围

该标准规定了计算机站场地的安全要求，适用于各类地面计算机站。不建站的地面计算机机房、改建的计算机机房、非地面计算机机房参照此标准执行。

3.2.2　相关术语

- 计算站场地：计算机系统的安置地点，机供电、空调以及该系统维修的工作场所。
- 计算机机房：是计算站场地最主要的房间，放置计算机系统主要设备的地点。
- 非燃烧材料：指材料受燃烧或高温时，不起火、不微燃、不碳化、只软化的材料。
- 难燃烧材料：指材料受到燃烧或高温作用时，难起火、难微燃、难碳化的材料。
- 活动地板：是指计算机机房内安装的、可灵活装拆的地板。
- 温感探测器：指在物质燃烧时，使周围空气温度升高致使发生报警信号的装置。
- 烟感探测器：指物质因燃烧或发热而分解生成的烟雾致使发出报警信号的装置。
- 应急断电装置：指机房发生意外事件时，能立刻切断计算机系统供电电源的装置。
- 接地：指系统的直流、交流工作地、安全保护地和防雷保护地与大地之间的连接。
- 二次破坏：指为了消灭火灾而采取的方法不当，造成对设备、信息等的再次破坏。
- 安全区：指采取安全措施能达到的有效区域。

3.2.3　计算机机房的安全分类

1. 计算机机房的安全类别

根据标准 GB9361—1988 计算机机房的安全分为 A 级、B 级、C 级三个基本级别。把要求具有最高安全性、可靠性的系统应实施的内容定为 A 级安全机房，A 级对计算机机房的安全有严格的要求，有完善的安全措施；C 级则是为确保系统做一般性运行时要求的最低限度的安全性、可靠性所应实施的内容，C 级对计算机机房的安全有基本的要求，有基本的计算机机房安全措施；介于 A 级和 C 级之间的是 B 级，B 级对计算机机房的安全有较严格的要求，有较为完善的计算机机房安全措施。

2. 计算机机房的安全要求

国家标准 GB9361—1988 对计算机机房的安全要求根据机房的安全级别而有所不同，具体内容如表 3-1 所示。

表 3-1　计算机机房的安全要求

机房安全类别指标 / 安全项目	C 类安全机房	B 类安全机房	A 类安全机房
场地选择	–	+	+
防火	+	+	+
内部装修	–	+	–
供配电系统	+	+	–
空调系统	+	+	–
火灾报警及消防设施	+	+	–
防水	–	+	–
防静电	–	+	–
防雷击	–	+	–
防鼠害	–	+	–
电磁波的防护	–	+	–

3. 安全执行策略

根据计算机机房安全的要求，机房安全可按某一类执行，也可按某些类综合执行。

3.2.4　场地的选择

在建立计算机机房场地的初始阶段，选择符合安全标准的场地是头等重要的因素，国家标准对如何选择符合各安全等级的机房的场地有明确的规定。

1. B 类安全机房的选址要求

- 应避开易发生火灾危险程度高的区域。
- 应避开尘埃、有害气体来源以及存放腐蚀、易燃、易爆物品的地方。
- 应避开低洼、潮湿、落雷区域和地震频繁的地方。
- 应避开强振动源和强噪声源。
- 应避开强电磁场的干扰。
- 应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
- 应避开重盐害地区。

2. C 类安全机房的选址要求

参照 B 类各条执行，如果有特殊要求，各部门单位将另行指出。

3. A 类安全机房的选址要求

A 类安全机房除要满足 B 类各种要求外，还应将其置于建筑物安全区内。

3.2.5　结构防火

建造计算机机房时应考虑到防备各类自然灾害，其中最典型的就是防止火灾问题。计算机机房起火的原因一般有以下几点：外部房间起火后蔓延到机房；技术和管理上的疏忽；人为的不慎引起火灾。计算机机房对于结构防火有一定的要求。

3.2.6　计算机机房内部装修

国家标准 GB9361—1988 对计算机机房的安全要求中，对机房内部的装修也做出了相应的规定。

1. A、B 类安全机房应符合的要求

1) 计算机机房装修材料

计算机机房装修材料应符合 TJ16 中规定的难燃材料和非燃材料，应能防潮、吸音、不起尘、抗静电等。

2) 活动地板

标准中对机房需要使用的活动地板也提出了相应的要求。

2. C 类安全机房应符合的要求

参照 A、B 类执行。

3.2.7　计算机机房专用设备

此外，该标准对机房的安全要求中，也包括了对一些机房专用设备的安全标准。

1. 供配电系统

电源质量对计算机可靠运行的影响很大。为计算机提供的电源质量的好坏，直接影响着

计算机的可靠运行。发生电源故障可能会导致以下毁坏性的后果：数据全部丢失；输入和输出逻辑出错；影响中央处理机的性能；计算机失去瞬息记忆；短路中央处理机的内部电路；电源过载引起中央处理机内电气燃烧等。

1) A、B 类安全机房应符合的要求

- 计算机站应设专用可靠的供电线路。
- 计算机系统的电源设备应提供稳定可靠的电源。
- 供电电源设备的容量应具有一定的余量。
- 供电电源技术指标应按 GB2887《计算站场地技术要求》中第 9 章的规定执行。
- 独立配电时宜采用干式变压器。安装油浸式变压器时应符合 GBJ232 中的规定。
- 使用的电缆除应符合 GBJ232 中配线工程中的规定外，载流量应减少 50%。
- 计算机系统用的分电盘应放置在计算机机房内，并应采取防触电措施。
- 从盘到计算机系统的各种设备的电缆应为耐燃铜芯屏蔽的电缆。
- 设备走线不得与空调设备、电源设备的无电磁屏蔽的走线平行。
- 应选用铜芯电缆，严禁铜、铝混用，若不能避免时，应采用铜铝过渡头连接。
- 计算机电源系统的所有接点均应镀铅锡处理，冷压连接。
- 在计算机机房出入口处或值班室，应设置应急电话和应急断电装置。
- 计算机站场地宜采用封闭式蓄电池。
- 使用半封闭式或开启式蓄电池时，应设专用房间。
- 房间墙壁、地板表面应做防腐蚀处理，并设置防爆灯、防爆开关和排风装置。
- 接地应采用专用地线，专用地线的引线应和大楼的钢筋网及各种金属管道绝缘。
- 几种接地技术要求及诸地之间的相互关系应符合 GB2887 中的规定。
- 计算机机房应安装有应急照明和安全口的指示灯。

2) C 类安全机房应符合的要求

应满足 GB2887 中规定的三类供电要求。

2. 空调系统

机房空调是保证计算机系统正常工作的重要手段之一。通过空调调节机房温度、湿度和洁净度，为计算机设备创造良好的运行环境。

1) A、B 类计算机机房应符合的要求

- 采用专用空调设备，若与其他系统共用，应保证空调效果并采取防火措施。
- 空调系统的主要设备应有备份，空调设备在能量上应有一定的余量。
- 尽量采用风冷式空调设备，空调设备的室外部分应安装在便于维修和安全的地方。
- 电加热器和加湿器应有防火护衬，并尽可能使电器远离易燃材料制成的空气过滤器。
- 空调设备的隔热材料应采用难燃材料或非燃材料。
- 安装在活动地板上及吊顶上的送、回风口应采用难燃材料或非燃材料。
- 新风系统应安装空气过滤器，新风设备主体部分应采用难燃材料或非燃材料。

- 采用水冷式空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。

2) C 类安全机房的环境条件

应满足计算机厂家关于安装环境中的对空调系统的技术要求。

3. 其他设备和辅助材料

除了上述一些设备、材料外，根据不同的需要，不同机房也许会有各自不同的辅助设备和材料，对这些设备和辅助性材料的选择，该准则也提出了几点注意事项。

- 使用的辅助设备应是难燃材料和非燃材料，应采取防火、防潮、防磁、防静电措施。
- 计算机机房应尽量不使用地毯。
- 计算机机房内所使用的纸、磁带和胶卷等易燃物品要放置于金属制的防火柜内。
- 窗帘和屏风应选用难燃材料或非燃材料。

3.2.8　火灾报警及消防设施

此外，不能忽略的一个要点是：符合安全标准的机房，应该配备基本的火警和消防设施。

- A、B 类安全机房应设置火灾报警装置。
- A 类安全机房应设置卤代烷 1211、1301 消防系统，卤代烷 1211、1301 灭火器。
- B 类安全机房在条件许可的情况下，应设置 1211、1301 消防系统，并备灭火器。
- C 类安全机房内应设置卤代烷 1211 或 1301 灭火器。
- 除纸介质等易燃物质外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

3.2.9　其他防护和安全管理

1. 防水

除了防火外，人们想到的第一个安全防范措施往往就是防水，对机房安全的要求当然不能少了相关的规定。

- 有暖气装置的计算机机房，沿机房地面周围应设排水沟，应注意对暖气管道进行定期检查和维修。通往机房地沟的墙壁或是地面应该能防水渗透。
- 位于用水设备下层的计算机机房，应在吊顶上设防水层，并设漏水检查装置。
- 已设在地下室的机房，必须设有水泵和带检验阀的排水管和水淹报警装置。

2. 防静电

计算机机房的防静电技术属于机房安全防范范畴的一部分。由于种种原因而产生的静电，是发生最频繁、最难消除的危害之一。静电不仅会使计算机运行出现随机故障，而且还会导致某些元器件，如 CMOS、MOS 电路，双极性电路等的击穿和毁坏。此外，还会影响操作人员和维护人员的正常工作和身心健康。

静电的产生和静电带电：静电放电可形成火源引起火灾。由带静电的人体或是由带静电的物体向人体放电，在人体内有电流通过，会产生“静电单击”。

静电对计算机的影响，主要体现在静电对半导体器件的影响上。可以说半导体器件对静电的敏感，也就是计算机对静电的敏感。静电对电子计算机的影响表现有两种类型。一种是元件损害，一种是引起计算机误动作或运算错误。

元件损害主要是指用于计算机的中、大规模集成电路的损害，另外，对双极性电路也有一定的影响。对于早期的 MOS 电路，当静电带电体(通常静电电压很高)触及 MOS 电路管脚时，静电带电体对其放电，使 MOS 电路击穿。

3. 防雷击

除了防火、防水之外，人们日常生活中经常会遇到的一个自然灾害也许就是雷。国家对计算机机房安全的要求当中也考虑到了如何防止雷击的问题。

- 计算机机房应符合 GB157《建筑防雷设计规范》中的防雷措施。
- 在雷电频繁区域，应装设浪涌电压吸收装置。

4. 防鼠害

不少计算机用户遇到过这样的情况，网线或各种计算机外设的连线，不知何时被咬断了，上面留着一些齿印，人们首先想到的往往是鼠。国家对计算机机房的安全标准里也涉及这方面的内容：

- 在易受鼠害的场所，机房内的电缆和电线上应涂敷驱鼠药剂。
- 计算机机房内应设置捕鼠或驱鼠装置。

5. 防电磁波

如果附近有大的电磁场，会严重影响到计算机机房设备的正常工作和使用寿命，因此，对这一类的防护也被包括在国家机房安全标准当中。

- A、B 类安全机房电磁场干扰环境场强应满足 GB2887 中的有关要求。
- 在安全区边界由计算机辐射而产生的电磁场强度不应大于有关标准的规定。

3.3　设 备 安 全

计算机网络安全所面临的威胁分为两种：一是对数据的威胁；二是对设备的威胁。无论用户拥有的是一台计算机设备，还是由一套计算机设备组成的网络，设备安全的基本原理都是相通的。最显而易见的一点，就是通过物理隔离的方法实现对计算机设备及网络的安全保护。

国家保密局 2000 年 1 月 1 日颁布实施的《计算机信息系统国际联网保密管理规定》第二章第六条规定：“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。”

所谓“物理隔离”是指内部网不直接或间接地连接公共网。物理安全的目的是保护路由器、工作站、网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击。

在实行物理隔离之前，我们对网络的信息安全有许多措施，如在网络中增加防火墙、防病毒系统，对网络进行入侵检测、漏洞扫描等。

下面从计算机硬件安全、磁介质安全、信息加密解密、硬盘锁等方面进一步讨论设备安全的有关问题。

3.3.1　计算机硬件物理安全

计算机设备的体积，随着中央处理器的运算速度越来越快而变得越来越小，因此也导致了计算机硬件设备被移动的可能性越来越大，安全性越来越差。

1. 固定设备

固定硬件设备是指将计算机固定在桌子或其他物体上，一般是不能被移动的物体，这使得计算机无法随便被移动。这类装置很简单实用，特别是对台式计算机而言。

2. 给设备加锁

锁可以防止无关人员擅自打开计算机，从机箱内部拆卸配件。

最简单实用的办法可以考虑配置一个专用的计算机柜，平时是一个工作台，工作结束离开以后，把设备锁在柜子里。

另一种可以考虑的方法是安装电子报警系统，一张 IC 卡插在计算机设备里，它能在机器断开电源而移动的时候发出高分贝的报警声，这样能加强对必须不间断工作的计算机设备的安全防范。

3. 给设备加标签

给计算机加上标签是一个不错的方法，在失窃后可以帮助侦破工作，尽快找回失物。

目前还有一些新的标签方法，在机器上喷洒一种特殊的化学成分形成的涂层，利用该化学成分作为特殊的标识。某些此类标签甚至很难被涂改、擦除，更高级的甚至是隐形的必须通过某种化学成分的处理才能显现。当然，越复杂的技术和服务，价格也越高。用户可以根据实际需要，选择适合本身的特殊环境的产品。

4. 访问控制

早期的计算机用的最多的存储介质是磁盘，使用频率很高的输入输出设备是软驱。软驱锁可以有效地防止其他人使用引导盘或病毒源盘非法访问计算机，导致病毒感染计算机里的文件，或者破坏数据甚至硬件。

某些销售商可以提供特殊的软件盘，类似加密狗，这些盘有非常高的安全防范技术，没有这些盘，一般非法访问者无法读取计算机里的数据。

硬件驱动访问控制主要包括一张装在计算机里的卡，卡的硬件和某些应用软件配合使用，可以给计算机用户提供认证和授权访问文件的控制功能。

5. 不间断电源

UPS 是 Uninterruptible Power Supply 的英文缩写，翻译成中文就是不间断电源。当所有

电源都中断的时候，UPS 能立即将墙上插座供电切换到由其内部电池供电。UPS 有两个用途，一是帮助用户防止断电时候计算机立即掉电，丢失正在编辑的重要数据；二是为用户提供一个临时的电源，以便在必要的时候而又没有供电的情况下短时间维持计算机的正常工作。

6. 防止静电

静电对计算机而言是一个大祸害，它的破坏力犹如地震对建筑物一样，危害非常大，消除静电是计算机机房建造和计算机设备使用过程中必须认真考虑的问题。如前文提到的，静电可以当做接地问题来解决，在接触计算机设备之前应先使自身接地，这样做能有效消除静电的影响。

7. 监听输入输出设备

某些技术型非法访问者也许会采用改造硬件设施来达到监听计算机的目的。其他经常被用作监听的设备有鼠标监听、软盘监听、无线网卡监听、显示器电磁泄漏，网络数据包截取等。在使用计算机时要注意防止这些设备被非法改造成一种监听的装置。

3.3.2　磁介质安全

磁介质在存储传递的过程中，很容易受到窃取、篡改、伪造、销毁等不法行为的威胁。

1. 软磁盘的构造

磁盘内部构造由很多个圆形盘片组成，每个盘片上有很多个同心圆，这些同心圆被称为磁道。每个磁道又可以分为若干个扇区，扇区可以理解成一个扇形的区域。各个磁道上的扇区数目是一致的，因此从里到外的磁道的扇区里的数据密度是不同的，很明显，内部磁道的数据密度会大于外部磁道的密度。

一般软磁盘的使用寿命为 2×10^6 次，最好的可以使用 1×10^7 次。5.25 英寸的软磁盘有一个孔，位于磁道的开头，这个孔被称为索引孔。孔的两边是前置区和后置区，前置区里包括索引地址标志(IAM)、索引地址标志同步区(SYNC)以及一些间隙(GAP)。一般 IBM 个人计算机都采用软扇区磁盘。

扇区的作用是将数据分组，一般扇区分为两个部分：ID 区和数据区。

ID 区只在格式化的时候写入一次，数据区包括同步区、标志区、数据和 CRC 区域。为了适应各种磁盘转速，在 ID 区和数据区之间还会插入一些间隙(GAP)。

为了提高效率，扇区分成若干的簇(Cluster)，每个簇包含一定数目的扇区。簇是存储磁盘文件的基本单元，每个簇包含的扇区数是在格式化时候指定的，之后除非重新格式化否则无法修改这个数目。每个簇有编号，每个扇区也有逻辑扇区号，簇号与扇区号有对应的关系，换算公式如下：

逻辑扇区号=(簇号－2)×(扇区数÷簇数)＋数据区起始扇区号

格式化后的磁盘分为四个部分：引导记录(Boot Record)区；文件分配表 FAT1、FAT2；文件目录区 ROOT；数据区 DATA。

1) 引导记录区

引导记录区占据逻辑扇区 0，用来存放磁盘 I/O 参数和 DOS 自举程序。

2) 文件分配表

对于 5.25 英寸低密度软磁盘来说，文件分配表占据逻辑扇区 1 到逻辑扇区 4，用来存储文件所占用的空间。在文件分配表中，每个文件占有簇构成一个链表。每个簇等于两个扇区。文件分配表有两个相同的拷贝，每个占用两个扇区。

3) 文件目录区

对于 5.25 英寸的软磁盘来说，文件目录区占据逻辑扇区 05H 到逻辑扇区 0BH，共 7 个扇区，用来存放磁盘上的文件目录。

4) 数据区

用户数据区占用逻辑扇区 0CH 开始之后的所有扇区，用来存放用户的文件和数据。对于根目录下的文件名和子目录，都分配一个 32 字节的目录登记项。

2. 硬盘分区

所谓分区，就是将硬盘分为一个或多个大小不等的区域，每个区域可以作为一个独立的逻辑盘，不同的分区可以安装不同的操作系统，例如在 C 盘安装 Windows 系统，而在 D 盘安装 UNIX，E 盘安装 Linux 等。每个分区都包含四个部分：引导代码、文件分配表、文件目录区和用户数据区。

3. 磁介质的处理和存储

计算机用户用来存储数据的最常用介质就是磁介质，如何妥善处理和保存这些存储了重要数据信息的磁介质是一个任何时候都不能忽视的问题。

1) 记录分类

为了给需要重点保护的数据记录提供必要的保护，同时对某些不重要的记录不多余的保护，有必要对文件记录进行分类。大致来说，数据记录可以分为关键性记录、重要记录、有用记录和不重要记录四类。

2) 记录复制

对于上述的关键性记录，都必须复制，复制品分散存放在安全地点。

机房内的数据是系统有效运行需要的最小数据，不必要的数据尽量不要放在机房内。机房外的记录、没有复制过的关键性和重要记录应该存放在防火的房间内，或放在能防火、防高温、防水、防地震、防电磁场保险的柜子里。

3) 磁带库、磁盘

对于磁盘和磁带库的访问应该严格限制，只有管理员和调度人员方可访问。为了便于查找和检索，详细的目录清单是必需的，且应该包含以下信息：文件所有者、卷系列号、文件名及其描述、作业或项目编号、建档日期和保留期限。从外部借来的资料应当用文件所有者、卷系列号、文件名和描述、接收日期和归还日期进行归类。

4) 文件库

文件库是所有当前系统文件、程序和操作用的文件和源程序文件的存储场所，数据管理

部门负责扩充和检索存在这些文件中的资料。

对文件库的访问仅限于数据管理部门的人员。文件和数据常包含非常机密的信息，应当妥善保管和处理。

3.3.3　信息的加密和解密

对于计算机的磁盘，可以使用各种加密方法，使得某个磁盘只有合法用户才知道如何打开与使用。一般而言，磁盘信息加密可以分为目录项修改、修改 FAT 文件分配表、修改磁盘的其他信息、硬盘加密、特殊格式化等。

1. 目录项修改法

1) 修改文件名域

文件名域的第一个字节为某些特殊值时，具有特殊的含义。如：00H—标识目录部分的结尾，目录项尚未使用；E5H—标识文件已经被删除，以下的目录项仍然有效。可以把某些文件目录项的第一个字节改成 00H 或 E5H，这样用 DIR 命令或者资源管理器将不显示这些文件。

2) 改变文件属性

用 Debug 命令修改文件的属性项，例如改成 02 或者 01，文件属性改为隐藏或只读。

3) 修改起始簇号

将文件起始簇号，即文件目录项的第 1AH、1BH 字节，改成 0000，使该文件无法找到入口。

4) 其他方法

- 子目录加锁。在根目录下建立一个子目录，把要保护的文件拷入此目录，将此子目录的起始簇号改成 0000，这样子目录就上锁了。
- 建立循环子目录。在某个目录中建立下一级的子目录，修改子目录的数据重定向到该目录本身，形成死循环，使非法访问者无法进入真正的文件目录。
- 修改文件长度。自己记忆实际的文件长度，然后修改文件长度达到扰乱非法访问者视听的目的。
- 目录区的转移。将目录区移到其他位置，需要使用时再移回来。
- 文件目录区加密。对目录区内使用加密方法，例如异或运算，可以使得无法正常访问该目录。
- 卷标加密。对卷标进行加密算法，记录好原来的卷标，不知道如何解密的非法用户将遇到错误提示。

2. 修改 FAT 文件分配表

FAT 文件分配表当中包含很多重要的文件信息，通过修改相关的信息可以达到隐藏数据文件的目的。

- 改变文件在 FAT 表中的链接，他人就无法正常使用。
- FAT 表的移动，指将 FAT 表移动到其他位置。

- 文件簇号序列加密。

3. 修改磁盘的其他信息

"其他信息"包括 IDAM、DATAAM、ID、IDCRC、DATACRC 等。一般情况下，这些信息是看不到的，因为读取扇区时只显示 DATA 的内容。我们可以通过改变参数的方法，如原来的 N=2，亦即每扇区包含 512 个字节，把它改成 N=3 或者 N=4，每个扇区变成 1024 个字节或者 2048 个字节，这样上述的"其他信息"就变成了 DATA 的内容，就可以被看到并且修改了。

1) 修改 AM

AM 指 Address Mark(地址标识)，说明后面跟的数据段是什么内容，如 IDAM 的最后一个字节是 0FEH，意思就是标识下面的内容为 ID 标识。如果把 FE 改成其他的数值，则读写扇区的时候将找不到正确的扇区开始地址。

DATA AM 的最后一个字节为 0FBH，表示后面的 DATA 数据有效。如果是 0F8H，则表示后面的数据已经作废，复制时可以把作废的数据舍弃。

2) 隐含 ID

在一个正常格式化的磁道中，在某个数据场后面的间隙中人为地写上一个标识，内容随意，此标识可以当做"通行证"，核对正确则允许通过，不正确则显示错误提示信息。

3) 修改扇区的 IDCRC 和 DATACRC

每个扇区具有各自独立的 ID 和 DATA 奇偶校验数值，修改原本的 IDCRC 和 DATACRC，使不知道还原方法的用户无法访问磁盘扇区。

4. 硬盘加密

1) 修改活动分区指示符

每个硬盘都有一张分区表，分区表嵌在主引导记录中，用来记录硬盘分区的情况。一个分区对应分区表中的一个子项，每个子项在分区表中占据 16 个字节的空间。在这 16 个字节空间中有 1 个字节为系统指示字节，它的作用是指示该分区是否可用。

用 FDISK 程序对硬盘进行分区后，所有分区的系统指示均不为 0，表示这些分区可用。如果将某个分区的指示字节改为 0，机器重启后该分区就不可用。

根据这个原理，可以通过修改分区表中系统指示字节的值，来达到隐藏硬盘分区的目的。

将分区扇区中的活动分区指示符改为 00，使硬盘不能自举。也可以将系统指示符改为 00、01、04H、80H 以外的数值。

2) 修改分区有效标识

将分区结束标识符 AAH 改为其他的数值，这样修改后就不能用硬盘启动，用软盘启动后也不能进入硬盘。

3) 硬盘加锁

硬盘加密技术实际上就是给硬盘加锁，加锁后的硬盘只有用密匙开锁后才能使用。密匙有两种形式：一种是口令形式，密匙由授权用户掌握；另一种是密匙盘的形式，密匙盘掌握在授权的用户手中。硬盘加密技术主要采用以下几种方法。

- 为主引导扇区设置密码防拷贝。
- 利用文件首簇号防拷贝。
- 硬盘隐藏与还原技术。

5. 特殊格式化

1) 扇区软加密技术

扇区软标记加密方法很多，如扇区间隙加密法、扇区软指纹加密法、异常ID加密法、额外扇区加密法、超级扇区加密法、扇区错乱排序法、未格式化扇区法和扇区对齐技术等。

(1) 增加额外扇区

IBM个人计算机系列及其兼容机上所使用的5.25英寸双面密度软盘，每面40个磁道，每道9个扇区，每个扇区容量为512字节。在逻辑上，一个磁道包含若干个扇区以及前置区和后置区(GAP4)。前置区和后置区都是为了稳定电机或允许电机转速稍有偏差而设计的。

一般而言，前置区长度是固定的，为32个字节；后置区的长度是可变的，根据电机转速的不同而有所不同，一般有数百字节左右。在FM制下，每个扇区中不仅包含数据区(512字节)，还包含同步电机用的两个6字节的SYNC字符序列、4个字节的ID地址标志、1个字节的AMI、1个字节的数据标志或删除数据标志、两个2字节的CRC(ID域的CRC和数据区的CRC)、1个11字节的间隙(GAP2)和1个42字节的间隙(GAP3)。因此一个标准的扇区包含数据和一些必须的标志、间隙，共有587个字节。在MFM制下，一个标准扇区需要658个字节。如果我们要将9个扇区的磁道格式化成10个扇区，就必须修改磁盘的基数表，由于至少需要587个字节给第10个扇区使用，因此标准的9个扇区之间的间隔至少要缩小若干个字节，以空出来大于每个扇区包含的字节数的空间给第10个扇区。也就是：将每道的扇区数由09H改成0AH，扇区间的间隔长度50H改为0AH，即由原来的80个字节减少为10个字节，这样9个扇区之间空余出来的70×9=630个字节供第10个扇区使用。

(2) 超级扇区

超级扇区是指其长度接近一个磁道长度的扇区(如N=5，扇区长度为4096字节)。大于1024字节的扇区在写操作时容易出现问题，用普通的磁盘控制器不能写这些扇区，故可用专用设备在盘上写入一个超级扇区达到反拷贝的目的，但可以在程序控制下读出此超级扇区。

(3) 扇区乱序排列

磁盘都是软分段的方法规划(格式化)出来的。所谓软分段就是用扇区识别标志来存取磁盘上的信息，整个磁盘只有一个索引孔：这种磁盘的每个磁道上分布着固定数目的扇区，每个扇区的开始部分是扇区识别标志。一条磁道上的扇区从小到大按序排列，读写磁道扇区时，工具磁头号、磁道号和扇区号决定读写磁盘上的哪一个扇区。

一般情况下，磁道扇区号的排列是由小到大，从01排到09的。乱序排列是指扇区号由大到小排列，或跳跃式排列，甚至用大数排列等。

其格式化的方法与增加额外扇区的方法类似，只是要改变信息表。

(4) 未格式化扇区

对某个磁道的部分扇区不做格式化处理，如对某个磁道只格式化出6个扇区。

(5) 异常 ID 加密

每个扇区的 ID 值是在格式化时写入的，写入时不做正确性校验，所以格式化时写入的 ID 值可以为任意值。若格式化时写入的 ID 与扇区实际的磁道号、磁头号、扇区号不一致，就称为 ID 异常，它将导致格式化的扇区不能正确读写。同样盘上加密的文件中也需要一个程序来判断该位置的扇区是否为异常 ID，以此作为判断是否是原盘的依据，以防止非法拷贝盘被滥用。

由于格式化所需的 ID 参数是由指针 ES:BX 指定的地址，以磁道号 T、磁头号 H、扇区号 S 和扇区长度 N 四个字节为一组依次排列的，改变这些参数的顺序，就能格式化出特殊的磁道。

2) 磁道软加密技术

磁道软标记加密方法有：磁道接缝加密、额外磁道加密、宽磁道加密、未格式化磁道加密、磁道间距不规则变化加密和螺线型磁道加密等几种。

(1) 磁道的扩展技术

一般的磁盘机都可以正常读写 44 个磁道，所以在原来的 40 个磁道(0～27H 磁道)之外还可以增加几个磁道。将一些运行程序写入增加的磁道，做成原盘。在读取和运行时候，按照正常的方式读取 41～44 磁道的内容，读取文件的时候自然会有一个反馈信息，如果读取失败或者错误，说明读取的盘不是加密过的原盘。

(2) 未格式化磁道

在格式化磁道时，跳过某个或某些磁道，造成一个或多个未格式化的空白磁道，使被加密程序在系统下能正常工作，而传统的拷贝软件则无法正常拷贝，从而达到加密的目的，这就是未格式化磁道法的加密原理。使用加密程序时，首先利用在被加密程序中的一段特殊程序对磁盘进行校验，如果发现某一个(或一些)特定的磁道为未格式化的磁道，则磁盘为原盘，否则为非法拷贝。

3.3.4　硬盘锁

硬盘锁是为了防止硬盘被窃取后造成信息泄露。按照采用技术的不同，可以分为以下几种类别。

1. 硬盘锁分类

1) 热键式硬盘锁

热键式硬盘锁，顾名思义，就是将硬盘加上密码键保护，用户要使用计算机之前必须按下设置的密码键方可顺利进入计算机。这个程序的原理很简单，只要在原来的主引导扇区的代码里加入一段检查密码键是否按住的程序进行判断即可。

2) 密码式硬盘锁

密码式硬盘锁，顾名思义，就是将硬盘加上密码保护，用户使用计算机之前必须输入设置的密码方可顺利进入硬盘。这个程序也相对简单，只要在主引导扇区的代码内添加一段密码校验的程序进行判断即可。首先监听键盘输入，等待用户输入密码，不输入或者输入错误都不能顺利进入系统。

3) 硬盘隐藏程序

硬盘隐藏程序的目的，是使得通过软盘或光盘启动的系统不能识别硬盘，必须使用该硬盘启动才能顺利进入系统，并对硬盘进行读写操作。其主要原理在于修改硬盘分区表，在使用硬盘启动时，由于改写后的主引导扇区内的程序会将硬盘分区表恢复，因此可以顺利地读写硬盘，而用其他盘启动系统时因为分区表未恢复，所以不能正常使用硬盘。通常，使用异或的编码方法可以将分区表编码。

4) 隐藏式硬盘锁

在了解了上述的密码式硬盘锁和硬盘隐藏程序后，我们可以将这两种方法的核心程序合二为一，成为一个具备硬盘隐藏能力的硬盘锁。这个硬盘锁比之前的几个硬盘锁高明的地方在于它利用了使硬盘隐藏的技巧，使得非授权用户在不知情的情况下，因为不知道密码而无法正常访问硬盘，并且在用其他盘启动的时候也无法进入硬盘进行读写操作，更进一步强化了硬盘锁的保护功能。

5) 硬盘密码锁

硬盘锁用来防止未经授权的用户使用硬盘，它具有以下的特点。

- 启动时必须输入密码，密码须经过编码加密。
- 启动后硬盘进入写保护状态，用户不能读写；用热键输入密码后解除写保护状态。
- 具备防病毒防疫功能；可以随时撤除或改变密码而不对硬盘造成任何伤害。
- 可以将硬盘锁使用在自己的计算机上并将用户分为不同的等级。

6) 区域写保护式硬盘锁

区域写保护式硬盘锁用来防止未经许可的用户使用硬盘，和硬盘密码锁不同的是，它只针对硬盘的部分区域做写保护，而且在启动时不需要输入密码。

7) 写保护卡

保护硬盘的另一种方法是使用硬件的接口卡，与前面介绍的软件加密写保护的方法不同的是，硬件板卡的方式是将密码程序和写保护的程序都写入固化的 ROM BIOS 里，进一步加强了安全性，使得这部分程序不容易被修改、删除或感染病毒。计算机在启动时会对 640KB 核心内存以上的接口卡内存区做扫描，当发现在该区域内存有 AA、55H 这样的十六进制数值时，将以远程调用的方式跳转到指定的位置去执行该位置的程序。

8) 硬盘锁、写保护卡破解

一般破解此类接口卡式的硬盘写保护或数据加密卡的基本方式就是通过汇编 Debug 一步步进行跟踪，找出原始的中断 INT 13H 驱动器的进入点，将该中断 INT 13H 的位置改成加密前初始的中断位置。

2. 硬盘锁编程

1) 硬盘及主引导区知识

硬盘的主引导区是硬盘的物理地址的 0 磁头、0 柱面、1 扇区，大小为 512 字节，扇区头存放了一个引导程序，又称为主引导扇区记录(MBR)，中间存放的一段是 MBR 程序检测出错时使用的消息字符，前面的 446 个字节也可以完整地叫做 MBR，然后是大小为 64 字节的一个分区表，一共有四项，每项 16 个字节，记录着每个主分区的具体信息(包括某分区的

状态、分区的位置信息等)。主引导扇区的最后两个字节的内容是固定的，分别为 55H、AAH，这两个字节用来检测硬盘有效的标志位，如果这两个字节的内容被更改，那么系统引导时将报告找不到有效分区表。

2) 开机引导过程

计算机开机引导，通常要经过如下几个步骤。

(1) 启动电源开关。

(2) BIOS 自检，起始内存地址为 0FFFF:0000，检测各种硬件设备(包括显卡的 BIOS、内存等)。

(3) 将硬盘第一个扇区(0 磁头 0 磁道 1 扇区)读入内存地址 0000:7C00 处。

(4) 检查内存地址 0000:7DFE 处是否等于 0XAA55，若不等于，则转去尝试其他启动介质，如果没有其他启动设备，则显示相应的信息。

(5) 跳转到 0000:7C00 处执行 MBR 中的程序。

(6) MBR 首先将自己复制到 0000:0600 处，继续执行。

(7) 在主分区表中搜索标志为活动的分区。如果发现没有活动分区或有不止一个活动分区，则停止。

(8) 将活动分区的第一个扇区读入内存地址 0000:7C00 处。

(9) 检查 0000:7DFE 是否等于 0XAA55，若不等于，则提示“Missing Operating System”，然后停止或尝试其他启动盘方式启动。

(10) 跳转到 0000:7C00 处继续执行特定系统的启动程序，装入操作系统。

(11) 启动操作系统。

上述步骤中，前 5 步由 BIOS 的引导程序完成，后几步由 MBR 中的引导程序完成。

3) 硬盘锁原理

利用 BIOS 读取硬盘主引导扇区内容引导操作系统的机制，我们可以将原先的主引导扇区的内容保存到硬盘的一个隐蔽扇区，再将硬盘锁程序写入硬盘主引导扇区，在机器启动过程中，被替换的程序被读入内存，就运行了硬盘锁程序。

一般此类程序都用汇编语言编写，等待用户键盘输入口令，如口令正确则将事先备份好的原主引导扇区的内容读入内存 0000:7C00 处，将控制权交给原来的主引导扇区内的引导程序，就可以正常启动进入操作系统；如果口令错误，则循环等待用户输入口令，错误达到一定的次数则直接死机，或者进入死循环一直要求口令。

要破解此类硬盘锁，可以将原来的主引导扇区的内容写回硬盘主引导扇区的位置，并覆盖，然后重启机器。当然这样做的前提是具有对计算机的完全控制权。

4) 程序说明

一般而言，此类程序可以分为两个部分。

第一部分是口令识别程序，用汇编语言编写。通过编译、链接生成可执行的二进制代码程序，主要任务就是用来替代原先的硬盘主引导扇区引导程序，要求用户输入正确的口令。

第二部分是硬盘锁安装程序，该程序用来安装硬盘锁，把第一部分的内容写入主引导扇区的相应位置，把原先的主引导扇区的引导程序备份到其他扇区。

程序流程图如图 3-1 所示。

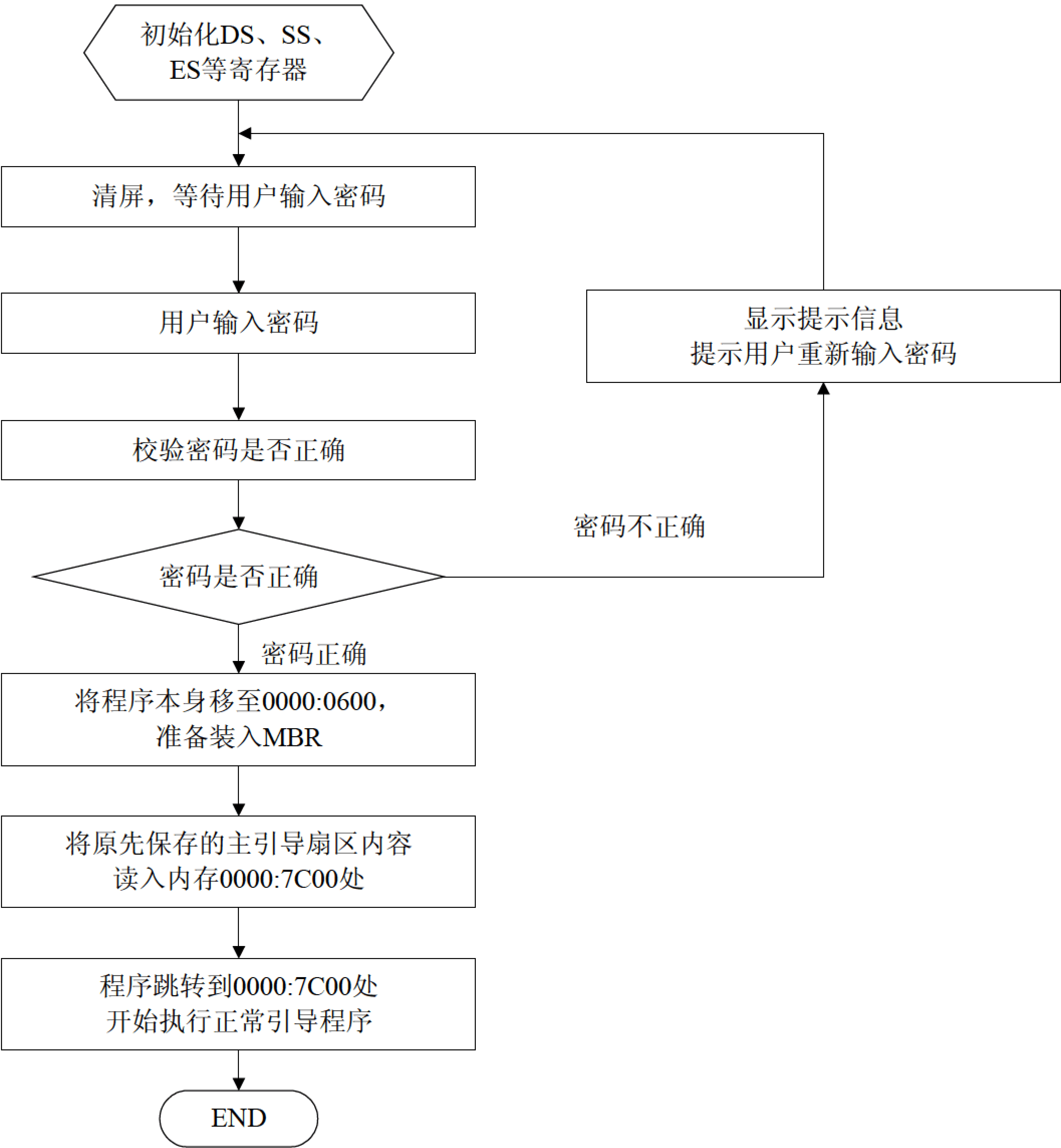


图 3-1　硬盘锁程序流程图

3.3.5　电磁辐射泄漏

利用计算设备的电磁波辐射窃取信息是目前国际情报机关窃取情报信息的重要手段之一。这严重威胁着计算机信息的安全，严重威胁着国家机密的安全。世界上一些发达国家对此问题引起了高度的重视，投入了大量的人力和财力解决。

一般会通过两种途径泄露计算机信息：一是通过辐射向外泄露，被称为辐射发射；二是传导泄露，也称为传导发射。前者指的是计算机内部产生的电磁辐射，后者指的是信息经过电源线、信号线、地线等向外传导造成的泄露。通常，起传导作用的电源线、地线等同时具有传导和辐射功能。我们可以采用以下多种方法对计算机设备的信息泄露加以保护。

1. 采用低辐射设备

这是防止计算机设备信息泄露的根本措施。

2. 距离保护

设备的电磁波辐射在空间传播时会随距离衰减，在距设备一定的距离外，设备信息辐射场强会变得微弱，这时就无法接收到辐射信号。

3. 噪声干扰

一是将一台能够产生噪音的干扰器放在计算机设备旁边，干扰器产生的噪声与计算机设备产生的辐射信息一起向外辐射，使计算机设备产生的辐射不易被区分。干扰器产生的电磁辐射不应该超过 EMI(Electro Magnetic Interference，电磁干扰)标准。

二是将处理重要信息的计算机设备放在中间，四周放置处理一般信息的计算机设备。采用这样的方法可以降低辐射信息被接收的可能性。

4. 屏蔽

将计算机设备放在具有一定屏蔽效果的屏蔽空间或屏蔽箱里，降低外部的信息辐射场强，这在一定程度上也可以降低辐射信息泄露的可能性。

3.3.6　IC 卡安全

IC 卡已经成为人们生活和学习当中随处可见的一项信息加密技术，这一节我们着重讨论与 IC 卡相关的安全问题。

1. IC 卡概述

IC 卡(Integrated Circuit Card)又称集成电路卡，也叫智能卡，它集成了超大规模集成电路，有各自的密码算法、编程算法，可以有定制的密匙，可以对文件加密，也可以对计算机加密，还可以对应用软件加密，防止被改。

智能卡的名称来源于英文单词“Smart Card”。它将一个集成电路芯片镶嵌于塑料片中，封装成卡片的形式，其外形与覆盖磁条的磁卡类似。IC 卡的概念是在 20 世纪 70 年代初提出的，法国的布尔公司(BULL)于 1976 年首先创造，将这项技术应用到金融、交通、医疗、身份证等多个行业，并将微电子技术和计算机技术紧密结合在一起。

1) IC 卡的分类

根据卡中所镶嵌的集成电路的不同，可以将 IC 卡分成以下三类。

- 存储器卡：可擦除的可编程只读存储器(EEPROM)，但不包含 CPU 中央处理芯片。
- 逻辑加密卡：卡中的集成电路具有加密逻辑和 ZEPROM，也不包含 CPU 芯片。
- CPU 卡：卡中的集成电路包括中央处理器 CPU、EEPROM、随机存储器(RAM)以及固化在只读存储器 ROM 中的芯片操作系统(Chip Operating System，COS)。

2) IC 卡的特点

与其他的数据存储和加密设备相比，IC 卡具有以下几个特点。

- 体积小，重量轻，抗干扰能力强。
- 便于携带，易于使用，方便保管。

- 安全性高，加密 IC 卡本身具有安全密码。
- 可靠性高，防磁，防静电，抗干扰能力强，可靠性比磁卡高，使用寿命长。
- 综合成本低，更加可靠，造价便宜，容易推广，维护方便，对网络要求不高。

目前，IC 卡家族中档次最高的是智能 IC 卡，即上面提到的 CPU 卡。这一类卡上不但有存储数据的存储器和对外联络的通讯接口，还带有具备数据处理能力的微处理器，实际上是一个卡上的单片微机系统。为了管理这一系统中的硬件和软件资源，卡上存储有进行数据读写和安全管理的程序，以及管理这些程序的卡上操作系统，即 COS。

COS 与计算机上常见的操作系统，如 DOS、Windows 等有很大的不同，它是针对 IC 卡的特点而设计的专用操作系统。COS 由于其上 IC 卡存储容量和微处理器性能而与常规的操作系统有很大的不同，其主要功能如下。

- 控制 IC 卡与外界的信息交换。
- 管理 IC 卡上各种存储器以及存储的方式。
- 在 IC 卡内执行来自 IC 卡读写器的各种操作命令，包括一些特殊的、面向具体应用的操作以及动态装载和卸载。

3) IC 卡的应用领域

IC 卡用途十分广泛，主要应用领域如下。

- 金融。世界上银行发行的信用卡绝大部分为磁卡，磁卡和 IC 卡比较，安全性差。
- 电信。数字蜂窝电话使用 CPU 卡存储信息和识别用户身份，这种智能卡通常被称为 SIM 卡。
- 电子钱包。专门针对小额支付而设计的，不需要电话确认、签名和密码，就可以支付日常的生活开支，如食品、交通、电话、电影等多种小数额支出。
- 政府。近年来，工商、税务、公安、海关、人事等部门也开始采用智能卡技术，提高办公效率。
- 公用事业。水、电、管道煤气、有线电视收费已有不少成功的应用智能卡实现预收费的实例。
- 交通。交通领域的特点使非接触式智能卡获得广泛的应用空间。
- 医疗。采用智能卡可以全面提高医疗诊断的效率、准确性以及管理水平。
- 社团、机构内部管理。一些综合性的应用，涉及的单位有企业、政府机构、机关、酒店、娱乐场所、旅游景点、居住小区和学校等。常用的功能有内部计费支付系统、购物消费、考勤等。

我国电子信息产业的发展，使得 IC 卡在行政管理、公用事业和银行业务方面得到了广泛的应用。目前我国已经成为世界 IC 卡发展最快的国家之一，各类 IC 卡的使用量达到两亿张。

2. 机卡分离式数字电视 IC 卡

机卡分离的数字电视是我国现阶段的数字电视方案，由机顶盒与电视机组成，其中机顶盒中使用了 IC 卡，可以进行条件接收。条件接收是数字电视衍生出来的增值业务，如视频点播 VOD、计量付费 PPV、软件下载、游戏、信息点播、数据广播等。

为了确保这些新兴业务的实现，需要使用条件接收系统(Conditional Access System，CAS)。有的有线电视系统中的 CA 是通过加密与授权的机制来控制信息的传送和接收。有线电视 CA 系统不仅可以控制用户的授权，还为用户提供一个安全的通道，使非授权者不能篡改他人传输的信息。

在客户端，可以通过机卡分离的数字电视机机顶盒完成上述功能。机卡分离是指机顶盒与 IC 卡的分离。

1) 机卡分离机顶盒的硬件系统

目前在国际上分离技术发展趋势之一是用 PCMCIA 卡解决问题，实现机卡的完全分离。

趋势之二是用智能卡技术实现卡和机身的分离。在技术上已经达到工业化批量生产，经济上也是完全可行的一个方案，基于智能卡的机卡分离技术将是一个发展趋势。

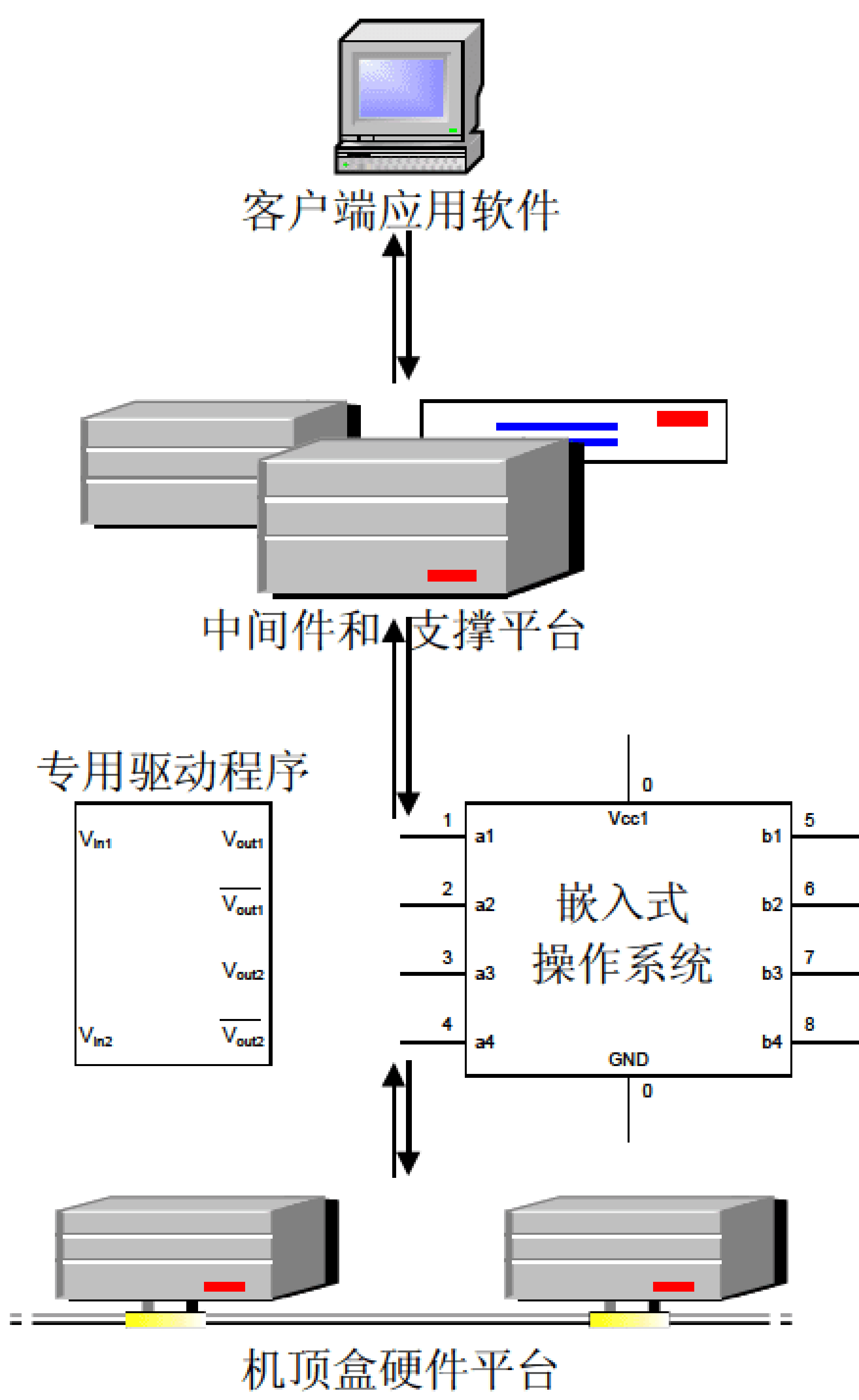


图 3-2　数字电视机机顶盒硬件系统

如图 3-2 所示，机卡分离的数字电视机机顶盒的硬件系统包括机卡分离机顶盒硬件平台、专用驱动软件、嵌入式的操作系统、支持机卡分离的中间插件及支撑平台，以及各种典型应用方面的客户端应用软件等部分。

2) 数字有线电视机机顶盒的硬件构造

上述的机顶盒硬件，主要包括 5 个部分，如图 3-3 所示。

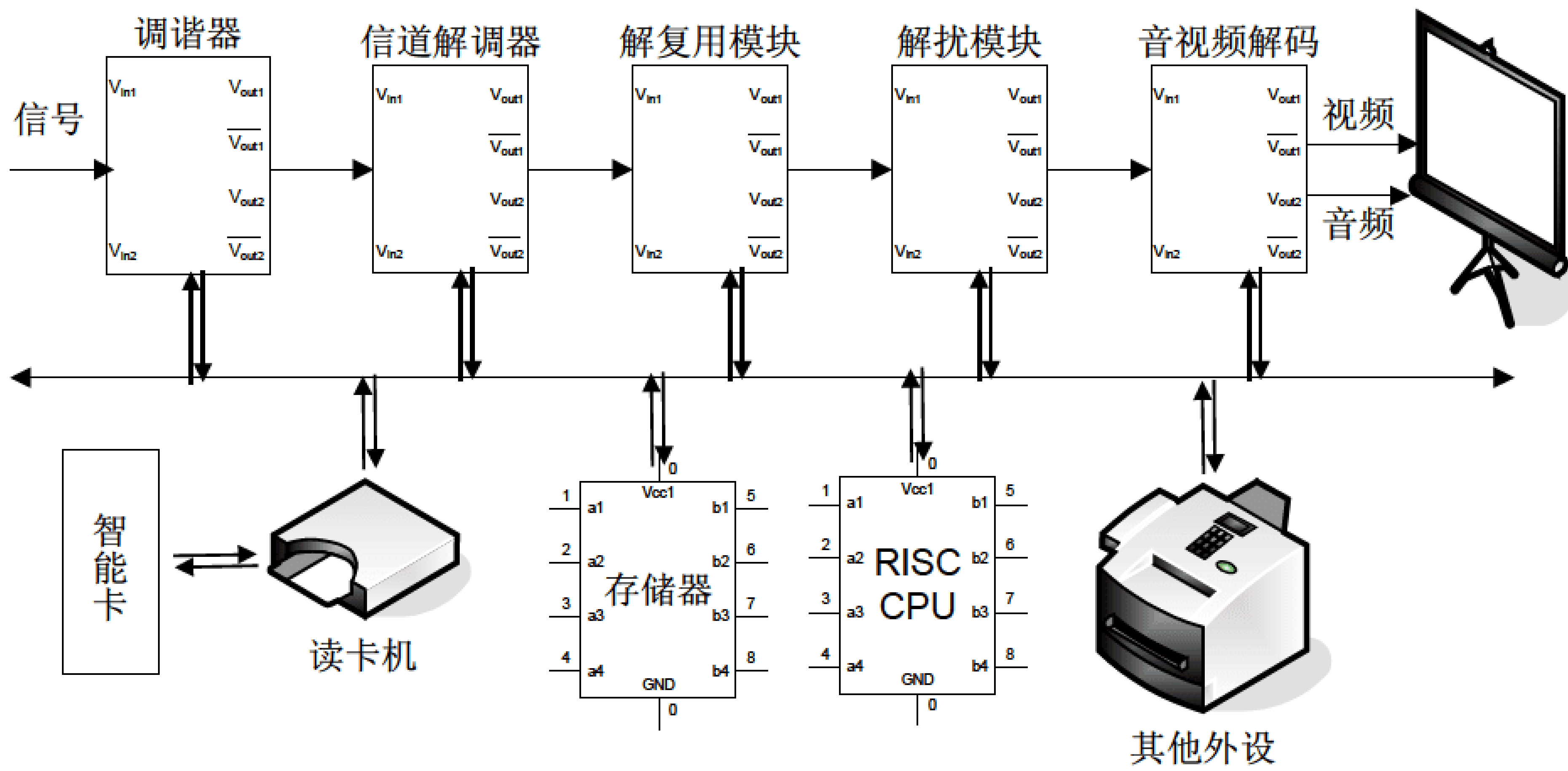


图 3-3　机顶盒的硬件平台

- 前端(包括调谐器和信道解码器)。
- 主控制器(包括 RISC 中央处理器、存储器 SDRAM 或 FLASH)。
- 解复用模块和解扰模块，完成 CA 在客户端使用时解密的过程。
- 条件接收智能卡模块。
- MPEG 音频、视频解码模块。

3) 支持 CA 的 IC 卡硬件体系结构

在机顶盒的硬件平台里，支持 CA 的 IC 智能卡的体系结构如图 3-4 所示。

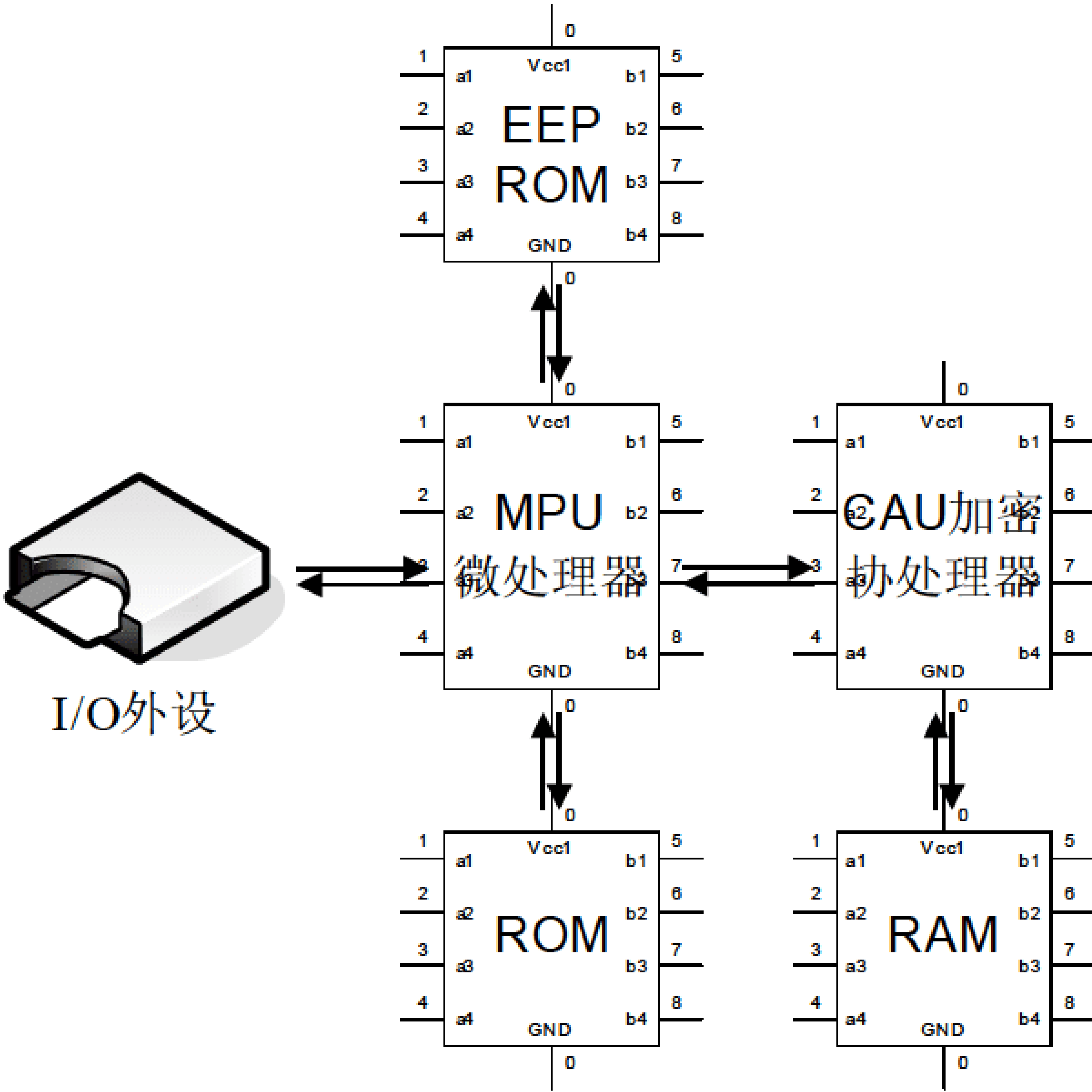


图 3-4　支持 CA 的 IC 卡硬件体系结构

此类 IC 卡的主要组成部分如下。

- 微处理器(MPU)负责系统的中央运算、数据处理、管理。
- 加密运算协处理器(CAU)执行有关加密解密运算的算法。
- 只读存储器(ROM)负责存储操作系统的程序代码。
- 随机存储器(RAM)负责工作过程中临时数据的存储。
- 电擦除存储器(EEPROM)负责应用程序、数据的存储。
- 通讯接口负责 I/O 外设与卡内部元器件的通讯传输。

除上述几个主要部分之外，可以视具体情况，加入一些保护内部软硬件的安全逻辑，此部分可以为硬件也可以是软件，由各开发商根据需要设计时定夺。

3.4　突发应急计划

应急计划一般由应急行动方案、资源备份、备份操作计划组成。应急计划应该包括操作系统中断、数据库和物理设备被破坏等情况的应急措施。应急计划是重要的计算机信息系统安全防卫措施，它可以被作为风险分析的辅助性手段去满足特殊部门的安全需求。

在应急计划中应该考虑的问题通常有以下几点。

- 紧急行动方案。紧急行动方案用于规范出现突发事件时，应首先采取的紧急处理措施步骤以及相关联系人。
- 资源备份。对于各种重要的信息资源，必须保持至少一份以上的备份。建议将重要的数据记录放到远程主机或数据库服务器中。
- 设备备份。在同一个现场使用两台相同的计算机，一台运行的情况下，另一台作为备份，备份机上应备份有完全相同的操作系统、程序、数据、文件。
- 备份操作计划。
- 恢复计划。恢复计划是指在设备部件失效、毁坏或数据丢失之后，对计算机系统进行快速恢复的实施计划。通常恢复计划应该包括数据恢复和设备恢复两个方面。

本 章 小 结

本章主要介绍了计算机物理安全的基本知识，包括：环境安全、计算机机房安全及等级、计算机实体设备安全、磁介质安全、信息加密和解密、硬盘锁、电磁辐射泄露以及 IC 卡安全等方面的内容。重点介绍了计算机站场地安全要求的国家标准 GB9361—1988，信息加密解密的程序流程，以及硬盘锁的技术实现和 IC 卡应用方面的相关内容。希望读者通过本章的学习能够掌握基本的计算机物理安全知识。

课 后 练 习

一、 填空题

1. 我国实行的计算机站场地安全要求的标准中将机房的安全等级分为(　　　　　)个等级。

2. 我国的国家标准里划分的安全等级，——(　　　　　)级的安全性最高，(　　　　　)级的安全级别最低。

3. 文件名域的第一个字节为某些特殊值时，具有特殊的含义。当它的值为(　　　　　)时，表明文件已经被删除。

4. 硬盘锁的原理是利用(　　　　　)引导操作系统的机制，将原先的(　　　　　)保存到一个隐蔽扇区，再将硬盘锁程序写入该区域。

5. IC 卡的全称是(　　　　　)，在 IC 卡家族中档次最高的是(　　　　　)卡，这一类卡不但有存储数据的(　　　　　)和对外联络的通讯接口，还带有具备数据处理能力的(　　　　　)。

二、 选择题

1. 在下述的安全项目里，按照我国的国家标准，建设 C 类安全等级的计算机机房，被

要求的项目是(　　)。

A. 防火　B. 空调　C. 消防报警　D. 防水

2. 下述(　　)不属于用特殊格式化法对扇区进行软加密的技术范围。

A. 扇区间隙加密　B. 软指纹加密　C. 超级扇区加密　D. 区域写保护

3. 下述(　　)不属于用硬盘锁的技术范围。

A. 热键式　B. 隐藏程序　C. 密码锁　D. 区域写保护

4. 下述对硬盘的主引导区的描述，正确的是(　　)。

A. 512 字节　B. 0 柱面　C. 0 扇区　D. 0 磁头

5. IC 卡可以划分的类别为(　　)。

A. 逻辑加密卡　B. 信用卡　C. 存储器卡　D. CPU 卡

三、 简答题

1. 简述我国实行的计算机站场地安全要求的标准所划分的安全等级及其主要特点。
2. 简述计算机站场地安全要求的标准对机房的选址要求，以及应该注意的事项。
3. 简述计算机硬件物理安全可以采用的主要方法。
4. 简述硬盘加锁可以采用的技术。
5. 简述 IC 卡相比磁卡所具有的优点。

第4章　操作系统安全基础

计算机操作系统是计算机系统配置的最重要的程序软件，在整个计算机系统软件中处于中心地位。操作系统设计的好坏，直接决定计算机系统的性能和计算机用户使用计算机的方便程度和安全性，操作系统的用户界面设计直接决定了该系统的人机接口友好程度。

目前个人计算机是世界上使用最多的电子设备，个人计算机上运行的操作系统主要有微软(Mircosoft)公司的 Windows 9x/ME、Windows XP/PE、Windows NT/2000、WindowsVista、Windows7 系列。UNIX/Linux 作为服务器操作系统平台也越来越被广泛采用。由于设计上的目标宗旨不同，Windows 9x/ME 等本身就不是为了网络应用设计的，甚至包括为网络应用设计的其他几个版本的 Windows，如 Windows NT/2000/XP 等，都存在不少的系统漏洞，造成了对用户计算机的安全威胁，很容易被一些带有不良企图的黑客攻击入侵。就连非 Windows 系列的 UNIX/Linux 等操作系统，也不能幸免于难。因此，计算机网络安全技术人员或计算机专业的高校学生，应了解这些系统的漏洞，加强安全管理，采取相应的防范措施，以保证系统安全、抵御非法入侵的攻击。

本章从上述的几个操作系统着手，讨论 Windows 系列操作系统以及 UNIX/Linux 等操作系统的安全基础、系统安全模型、管理、安全漏洞方面的问题。

本章重点

- Windows 操作系统
- Linux 操作系统
- UNIX 系统安全基础
- 操作系统漏洞
- 操作系统入侵检测

4.1　Windows 操作系统

4.1.1　Windows 操作系统简介

Windows 是目前在个人计算机上使用的最为广泛的操作系统。每天，全世界有数以十亿计的用户在使用微软公司出品的 Windows 系列操作系统。其中 Windows 9x 系列尤为值得一提，这是 Windows 家族里占据了绝大多数用户的操作系统市场的产品，Windows 9x 以其大

众化的友好界面及支持的众多应用程序赢得了广大个人计算机用户的青睐。与此相应，从Windows 9x开始的各个Windows版本也因此成为了黑客对普通计算机用户攻击的集中目标。Windows NT是微软公司第一个真正意义上的网络操作系统，它已经由NT 3.0、NT4.0发展到了NT 5.0，即俗称的Windows 2000，并逐步占据了广大的网络操作系统市场。之后推出的Windows XP、Vista，以及最新的Windows 7，进一步稳固了微软在个人计算机操作系统市场上的霸主地位。截止到笔者动笔之日，据不完全统计，Windows 7操作系统已经获得了全球范围内的几亿订单。

Windows操作系统在具有众多优点的同时，也具有十分明显的缺点，如稳定性和安全性欠佳。非网络操作系统系列的Windows 95/98等版本极易受到黑客的攻击和病毒的侵袭，一般网络用户使用一些软件工具，就可以轻而易举地让Windows 9x系统蓝屏或者死机。Windows NT在使用了与Windows 9x一脉相承的用户界面和友好的使用方法的前提下，加强了对网络应用和安全性的处理，对网络服务功能的支持更为完善和安全，稳定性也有了本质的提高。但是，也没有彻底消除操作系统漏洞对计算机和网络安全带来的隐患。因此在业界，有些人戏称微软的程序员都是裁缝工匠，每天都在为了各种系统漏洞"打补丁"，也因此而戏称Windows操作系统是满是补丁的不可靠的操作系统。

下面分别针对Windows 95/98/ME、Windows NT/2000/XP系统进一步介绍它们在安全方面的问题。

4.1.2　Windows操作系统安全体系结构

1. Windows 95/98/ME

由于Windows 95/98/Me本身就不是为网络应用设计的，因此它们存在许多安全性方面的问题，很容易被非法攻击。根据美国计算机安全中心(NCSC)公布的可信计算机系统评价准则(TCSEC，详见第2章相关章节的介绍)，Windows 95/98/ME等系统的安全等级只能达到D级，基本上相当于未加安全措施的个人计算机系统。

在了解Windows 95/98/ME系统的安全机制的基础上，可以通过修改注册表信息等方法来提高它的安全性。本节将以Windows 98为例简单介绍如何通过修改这些信息增强Windows 95/98/ME系统安全性。

1) Windows 98登录机制

Windows 98系统的登录方式有三种：Windows登录、Microsoft网络用户登录和Microsoft友好登录。Windows登录是指仅登录到本地Windows、不访问网络的登录方式，如果以前保存过个人设置，登录时会自动恢复。Microsoft网络用户登录是指登录以后可以访问网络资源，如果指定了域服务器，登录时会同时进行域身份验证。Microsoft友好登录是指登录时提供在本机登录过的用户列表，供用户选择并进行验证登录，方便和简化了用户操作，同样在登录以后就可以访问网络。

上述的三种方式，只有Microsoft网络用户登录和Microsoft友好登录这两种选项，要求Windows 98系统有网络适配器时才选择。以上三种登录方式各有特点，安全级别也各不相同。

(1) Windows 登录

这是 Windows 刚安装完成后默认的登录方式，也是 Windows 中最不安全的登录方式，Microsoft 公司设计的 Windows 登录机制的用意是：不同用户使用 Windows 98 系统时，各有一个自己的个性化桌面和菜单选项，而不在于保护系统和防止非法用户使用计算机。所以，在 Windows 98 启动后出现“欢迎使用 Windows”的登录对话框时，只需要单击“取消”按钮，即可进入系统，如图 4-1 所示。

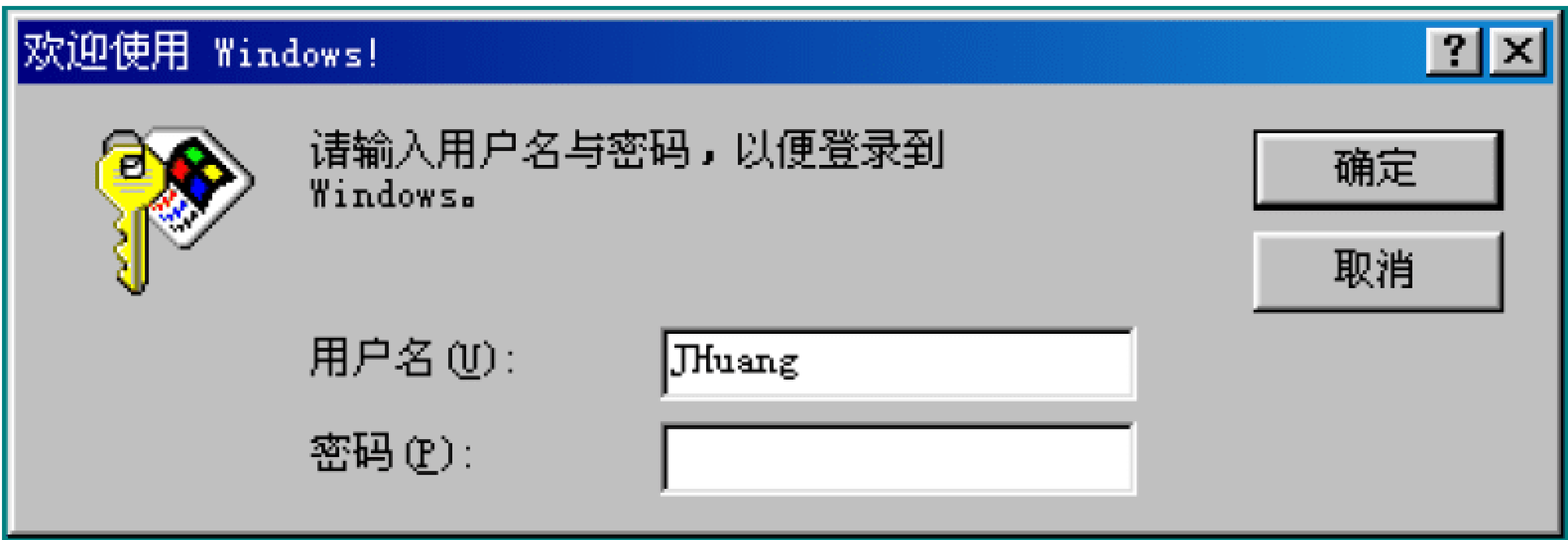


图 4-1　Windows 登录

(2) Microsoft 网络用户登录

要以此种方式登录，需要对“控制面板”中的网络属性进行修改，在“配置”选项卡中选择“推荐”，之后选择“客户”，然后设置 Microsoft 厂商和 Microsoft 网络用户，如图 4-2 所示。

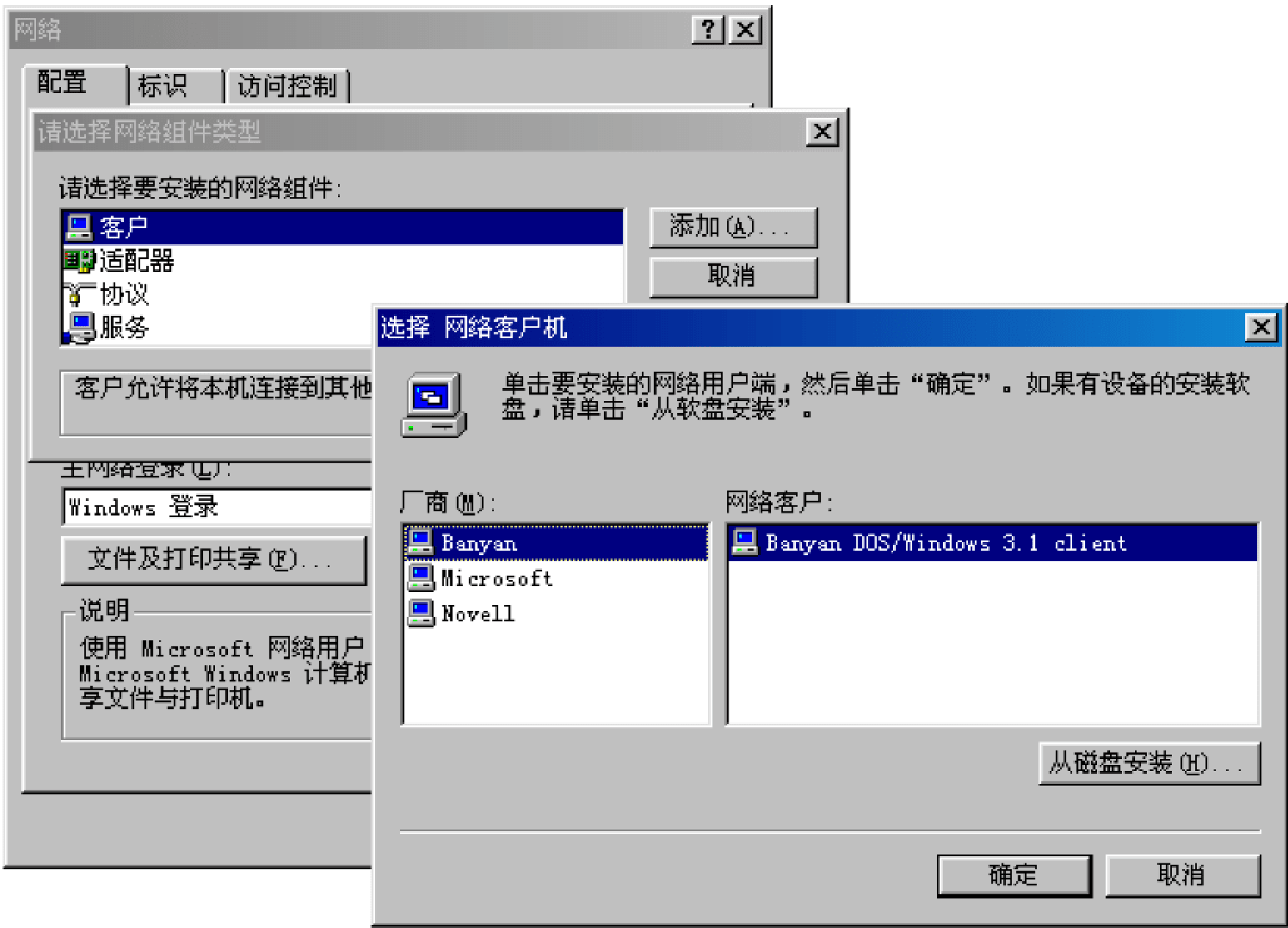


图 4-2　添加 Windows 网络用户

然后在“主网络登录”中选择“Windows 网络用户”，确定后重启计算机即可，如图 4-3 所示。



图 4-3　选择网络登录方式

不过进行这一步骤前，务必需要注意的是：计算机必须接入某个 Windows NT 网络，该服务器必须正在运行，并且必须是该 Windows NT 服务器上的一个合法用户，然后在出现登录网络对话框时输入在服务器上注册过的用户名、密码，如图 4-4 所示，最后单击“确定”按钮方可进入 Windows，否则会被拒之门外。

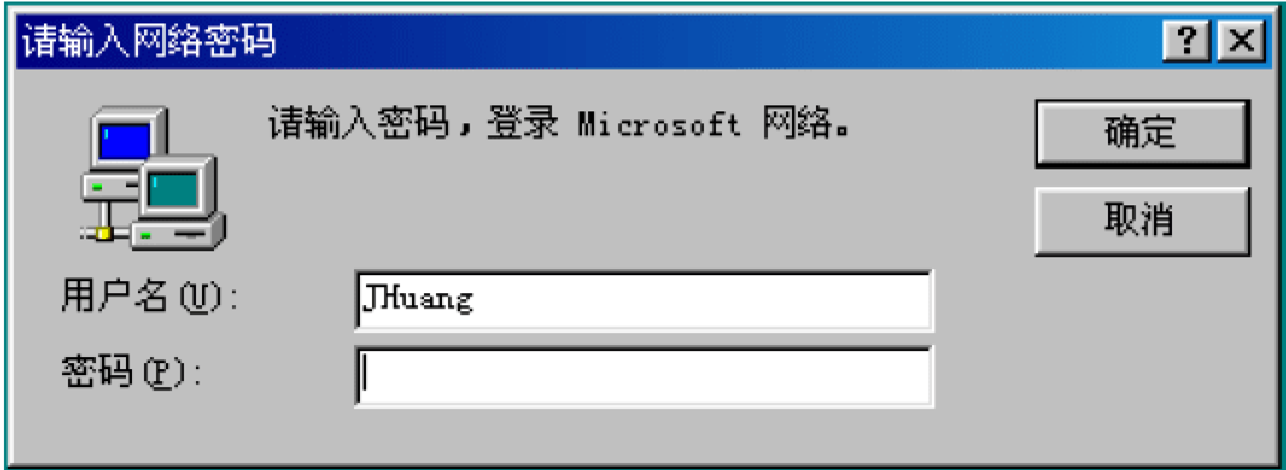


图 4-4　Microsoft 网络用户登录

(3) Microsoft 友好用户登录

要以此种方式登录，首先要在“控制面板”中对网络属性进行修改，在“配置”选项卡中选择“推荐”，之后选择“客户”，然后选择“Microsoft”和“Microsoft 友好登录”，如图 4-5 所示。

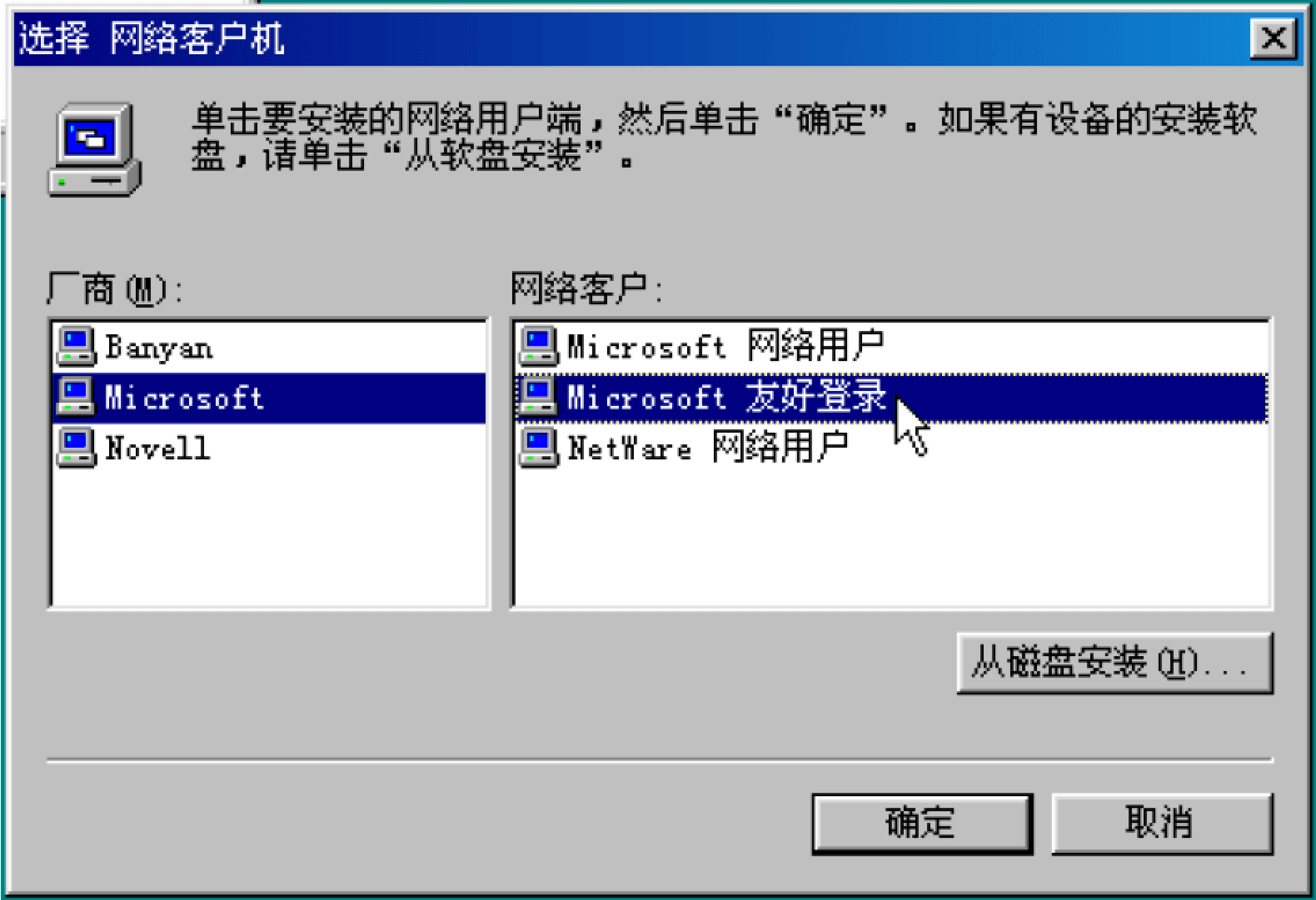


图 4-5　添加 Microsoft 友好登录方式

之后在主网络登录中选择“Windows 登录”或者“Microsoft 友好登录”，单击“确定”按钮后重启计算机。即可看到开机登录窗口列出的该计算机上的用户名，登录时先选择用户，如图 4-6 所示。



图 4-6　Microsoft 友好登录

然后在“密码”输入框中输入该用户创建时设置的密码，单击“确定”按钮。但是需要指出的是，这里的情况和 Windows 登录方式类似，如果单击“取消”按钮，也可以进入系统。要避免这样的毫无安全保护意义的登录方式，避免这样的现象发生，可以通过修改系统注册表来实现。具体做法见下文关于“利用注册表提高 Windows 95/98/ME 安全性”的介绍，这是一种相对比较安全的方法。

2) 利用注册表提高 Windows 95/98/ME 安全性

Windows 98 操作系统深受广大用户的喜爱，但是安全性方面的问题则使这个系统不让人放心。在这里我们需要指出的是，如果熟悉了这一个系统的特性以及安全相关的机制，仍可以为它创建一个相对安全的工作环境。这个相对安全的运行环境可以在一定程度上防止非法用户随意登录和操纵用户的计算机，这里我们将介绍如何通过修改注册表达到这样的目的。

众所周知，Windows 98 的注册表是一个庞大的数据库，其中存储了应用程序和计算机系统的全部配置信息，是 Windows 98 系统的核心内容之一。它存在 Windows 98 目录下的 System.dat 文件里，这是一个只读、隐藏的文件，每次系统启动时都要访问它，根据它内部的设置信息来加载各种服务和应用程序。所以，不论在任何时候，使用任何工具，对注册表进行修改操作之前，最好对注册表进行备份，以便在操作系统受到意外损坏以后可以恢复到修改前的状态。由此可见，它对整个 Windows 98 系统的安全运行起着十分重要的作用。

(1) 禁止非法用户登录

前面我们介绍了有关 Windows 98 的三种登录方式。其中在“Microsoft 友好登录”相关篇幅里提到，Windows 98 在启动和注销后，会要求用户输入用户名和密码，但是只要单击“取消”按钮，即可进入系统，并不能阻止非法用户的使用。那么有没有办法让这种毫无防范措施的系统阻止非法用户的进入呢？答案是肯定的。只要在 Windows 98 已有的安全机制的基础上，添加启动它的安全功能，就可以防止非法用户的登录。

首先，如上一节介绍的步骤进行操作，将登录方式改为“Microsoft 友好登录”。具体步骤为：打开“控制面板”，双击“网络”图标，出现对话框之后，在“网络”对话框中下方选择“主网络登录”，在出现的下拉列表中选择“Microsoft 友好登录”，然后单击“确定”

按钮，如图 4-7 所示。



图 4-7　选择“Microsoft 友好登录”

这样就把 Microsoft 友好登录设置成系统默认的登录方式，如果没有找到这个登录方式，说明没有添加该方式，请参照上一节的内容进行添加，如图 4-5 所示。在“网络”对话框中，打开“配置”选项卡，单击“添加”按钮，双击“客户”，在“厂商”列表中选择“Microsoft”，然后在右边的列表中选择“Microsoft 友好登录”，单击“确定”按钮。然后再按照图 4-7 所示选择主网络登录方式，完成后单击“确定”按钮就完成了设置。

需要注意的是，在添加这种客户登录的时候有可能需要插入 Windows 安装系统光盘，请务必保证盘在手边随时备用。

接下来，需要建立专门的用户，目的是方便使用计算机的用户设置新用户名和各自的密码，以便于保护每个用户的个性化桌面和菜单设置。具体方法为：在“控制面板”中，双击“用户”图标，在出现的“用户设置”对话框中，单击“新用户”按钮，给每个授权使用该计算机的用户建立独立的用户名，如图 4-8 所示。



图 4-8　添加新用户

设置一个默认的密码，等用户登录后自己修改密码，重新启动系统。设置完成后，无论

何时，用户使用该用户名和密码登录 Windows 98 时，都将得到自己个人定制的桌面图标、快捷方式、背景图片等个性化的界面。

最后，我们进入最主要的环节：修改注册表。为了安全起见，需要事先备份注册表。修改注册表的步骤如下。

① 打开注册表编辑器。

选择任务栏上的“开始”→“运行”菜单命令，在弹出的窗口中输入“regedit”，单击“确定”按钮，即可看到“注册表编辑器”窗口。

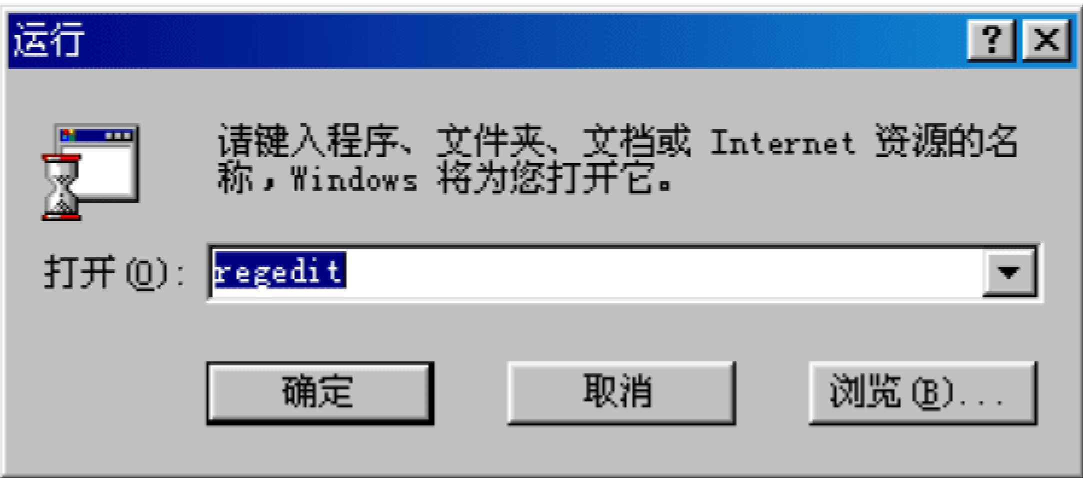


图 4-9　打开注册表编辑器

② 创建一个新的参数。

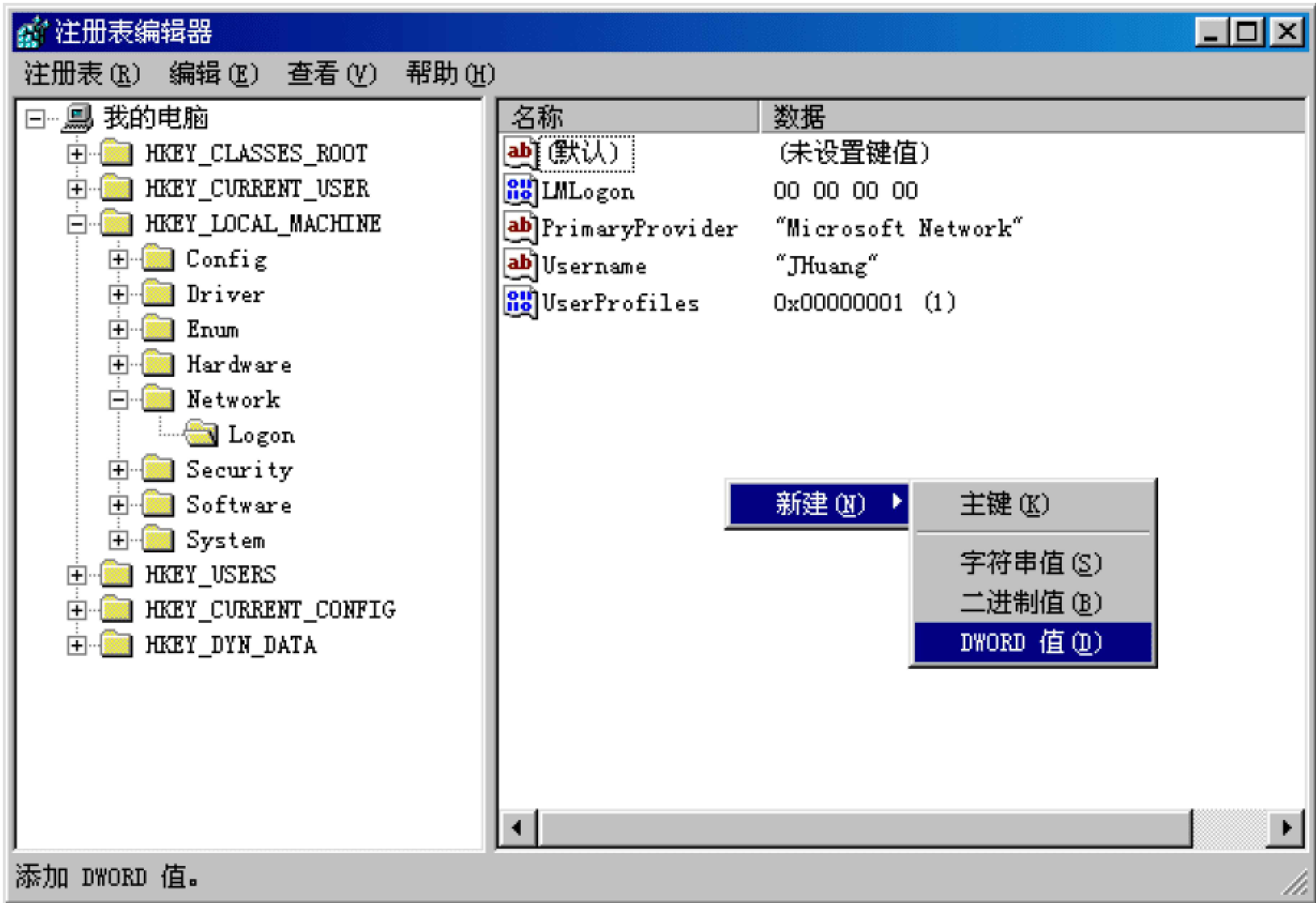


图 4-10　创建一个新的 DWORD 值

在注册表编辑器中，找到“HKEY_MACHINE\Network\Logon”，在该分支的右边窗口中创建一个 DWORD 值，名为“MustBeValidated”。创建 DWORD 值的方法是：在“注册表编辑器”右边的窗口空白处单击鼠标右键，出现“新建”菜单，选择其中的“DWORD 值”，如图 4-10 所示。

③ 为新创建的参数赋值。

将该参数“MustBevalidated”赋值为 1，如图 4-11 所示。

经过这样修改，在用户启动 Windows 98 之后，如果在登录对话框中单击“取消”按钮试图进入系统，系统将无法显示桌面。通过这样的方式，Windows 98 可以拒绝非法用户的登录使用，只有合法授权的计算机用户才能输入正确的用户名和密码进入系统进行使用。

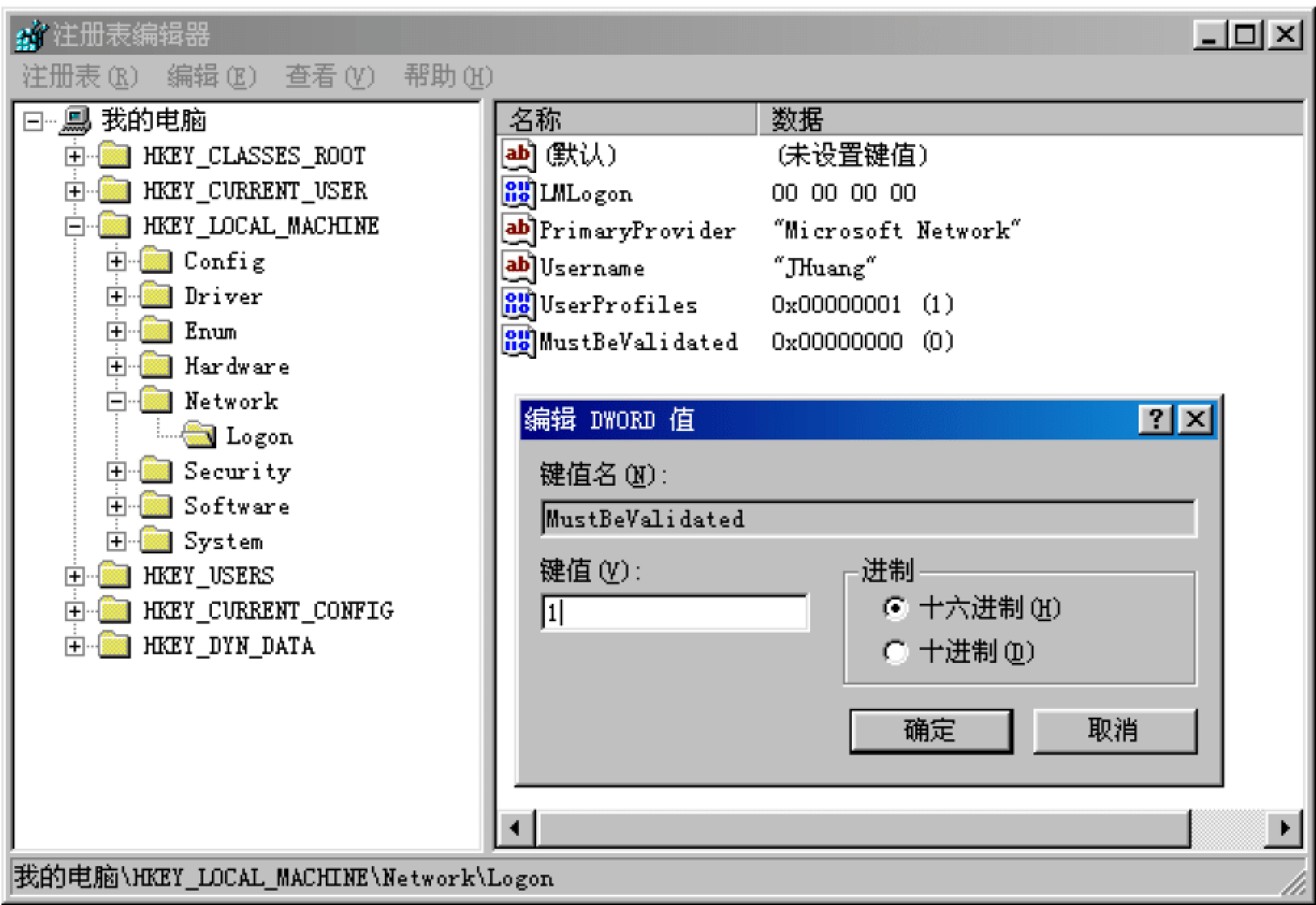


图 4-11　给新添加的参数赋值

为了给用户一个提示，让非法用户不必白费力气，就可以在登录窗口中添加一些提示信息。这一功能可以通过直接编辑系统注册表来实现，具体步骤为：运行 regedit.exe，打开“注册表编辑器”，选择“HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\WinLogon”(如果没有找到，就先创建)分支，在其右边新建一个字符串值，命名为“LegalNoticeCaption”，然后双击，把它的值设为提示信息的标题，比如，“提示信息”；再新建一个字符串值，改名为“legalNoticeText”，然后双击，把它的值设为提示信息的内容，比如“非法用户，请联系管理员获取合法账号！！！”，如图 4-12 所示。这样，提示信息就设置好了，然后重新启动计算机，如果登录非法就会提示如图 4-13 所示的信息。

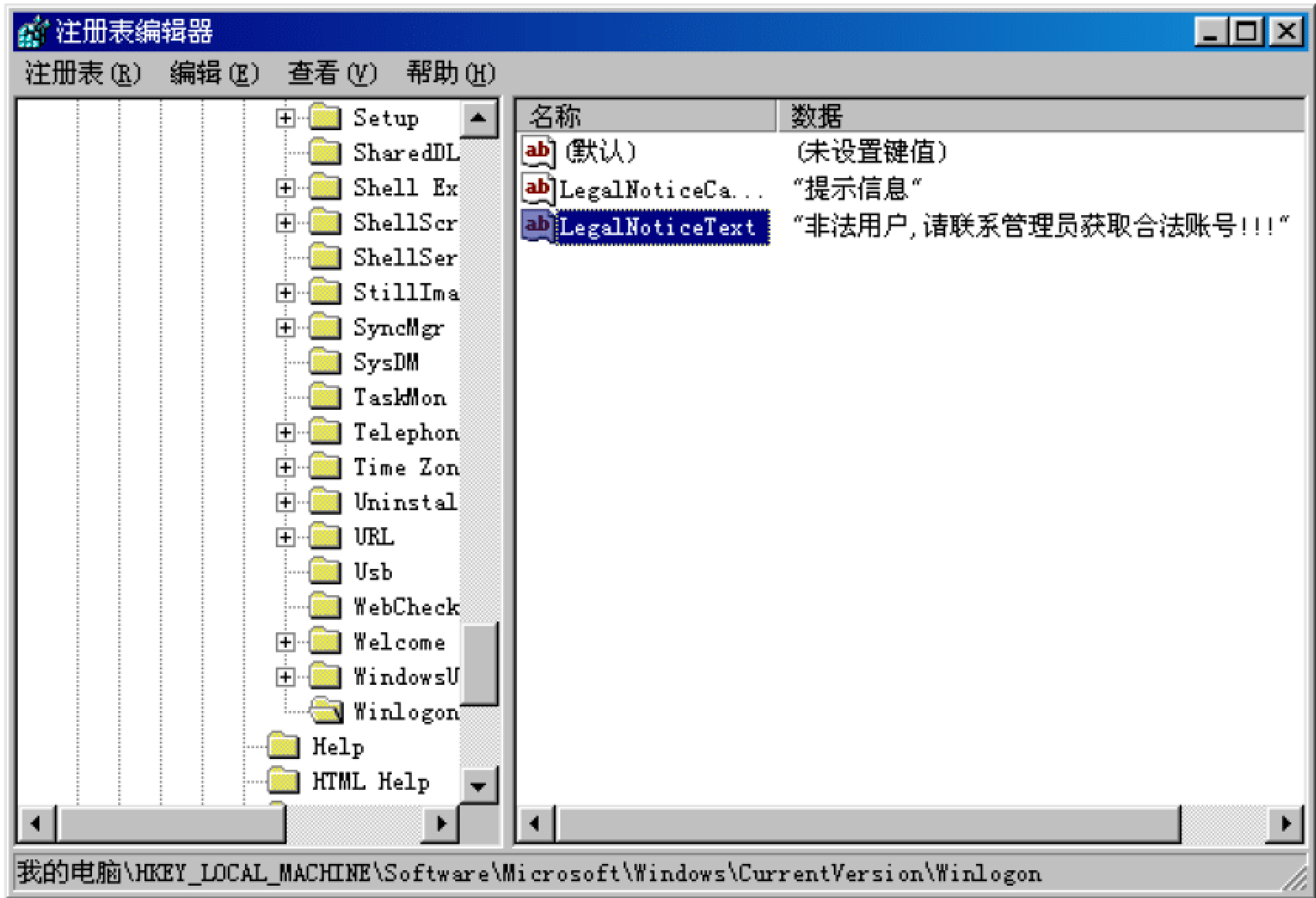


图 4-12　添加登录提示信息



图 4-13　非法登录

按照上面的方法设置后，还有一个问题：在登录 Windows 98 系统时，虽然每次登录都需要密码，但是上次登录的用户名总是出现在登录对话框里，因此，熟悉该用户的非法用户根据用户名有可能会猜中密码，尽管这样的几率很小，但是也是一个安全隐患，会对系统的安全造成威胁。那么有没有办法让 Windows 98 启动的时候，要求用户登录的界面上不显示

之前登录过的用户名呢？答案是肯定的。具体方法为：打开“注册表编辑器”，查找 HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\WinLogon 分支，如图 4-12 所示，在该分支的右边窗口中新建一个名字为“DontDisplayLastUserName”的 DWORD 值，双击，修改它的值为 1。这样在登录的对话框中就不会出现上次登录的用户名了。

(2) 隐藏“控制面板”

“控制面板”是 Windows 系统的控制中心，在控制面板中可以对设备属性、文件系统、安全口令等很多系统的关键内容进行修改。那么，如何防范系统的东西被随意更改呢？

首先，启动“注册表编辑器”，打开 HKEY_CURRENT_USER\Software\ Microsfot\Windows\ CurrentVersion\Policies\System 分支，在该分支的右边窗口里新建 DWORD 值“NoDispCPL”，将它的值修改为 1，如图 4-14 所示，最后重新启动，即可隐藏“控制面板”。

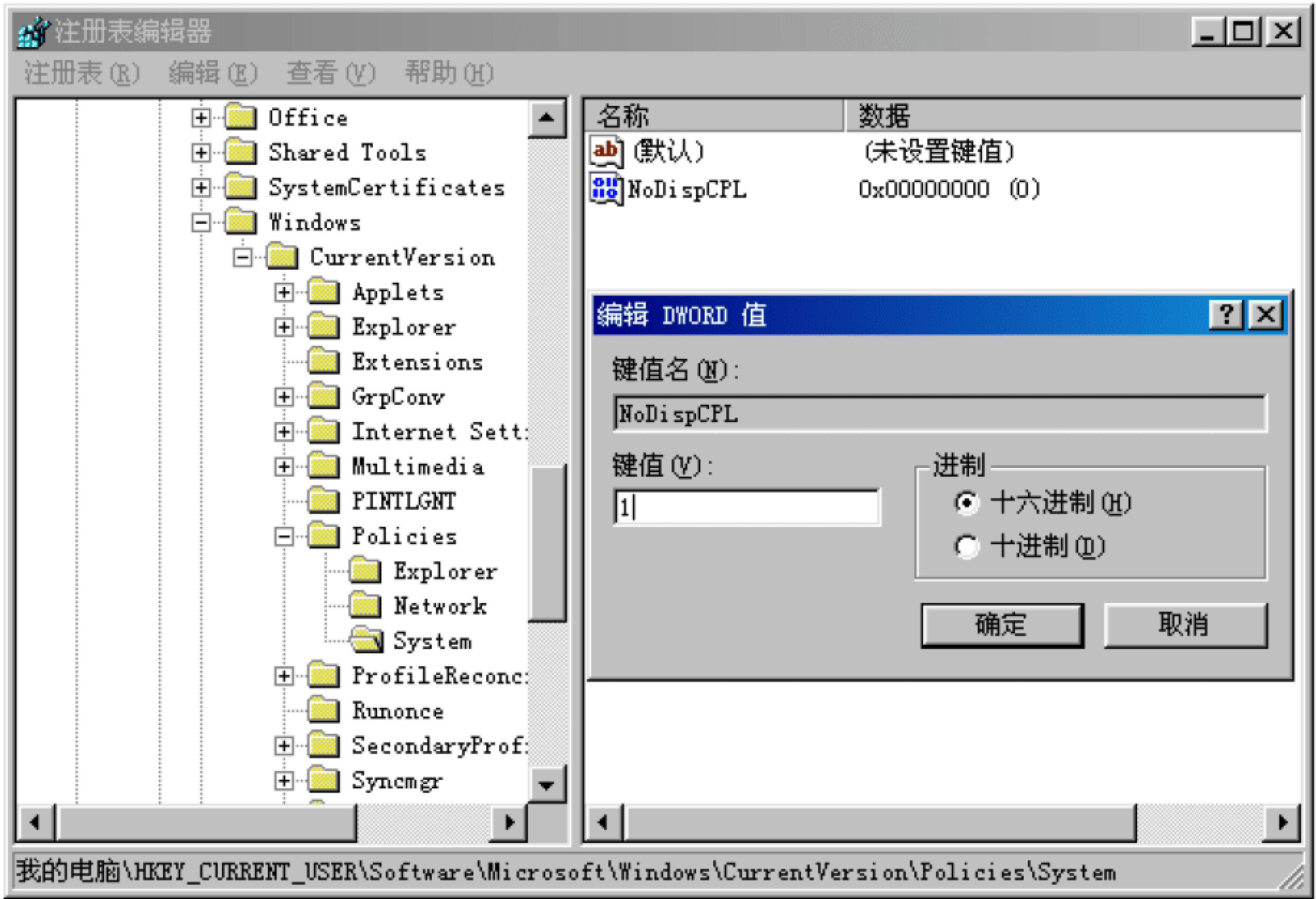


图 4-14　修改注册表禁止使用控制面板

(3) 禁用“注册表编辑器”编辑注册表

上面介绍了通过修改注册表可以禁止“非法用户登录系统”，禁止使用控制面板。我们又会遇到下一个问题，那就是：如果每次注册表信息都可以被用户修改，那么知道这个系统安全漏洞的用户可以通过修改注册表把这些信息改回去，又可以使非法用户随意登录系统。并且，注册表信息对于很多用户来说是相当复杂和危险的，尤其是初学者。为了安全起见，最好还可以禁止使用“注册表编辑器”来修改注册表信息。这一点，在公共机房显得尤为重要，因为一不小心系统的注册表就会被一个无知的用户破坏，或被改得面目全非，所以，禁止随意修改注册表是一项势在必行的安全措施。

禁用“注册表编辑器”编辑注册表的具体步骤为：启动“注册表编辑器”，打开 HKEY_CURRENT_USER\Software\Microsfot\Windows\CurrentVersion\Policies\System(如果发现 Policies 下面没有 System 主键，请在它下面新建一个主键，取名 System)，然后在右边的窗口处新建一个 DWORD 值，命名为“DisableRegistryTools”，把它赋值为 1，如图 4-15 所示，这样修改以后，不仅别人无法运行 regedit.exe 来编辑注册表，自己也不例外。那问题又摆在面前，如果要恢复对注册表的编辑修改功能，应该如何操作呢？

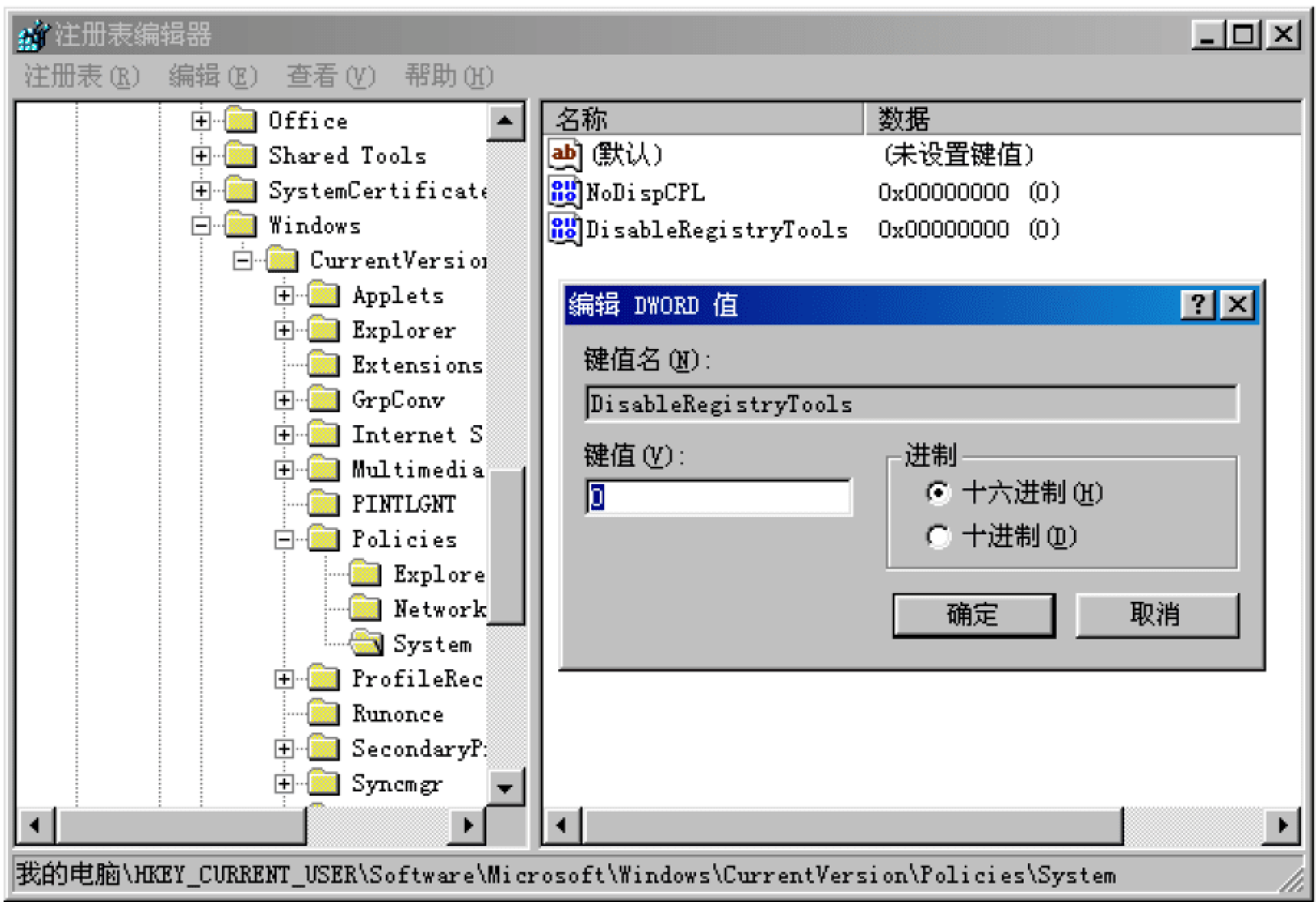


图 4-15　修改注册表禁止访问注册表编辑器

可以将下面的这一段代码用文本编辑器编辑保存，取名为 reg.reg，然后把它导入注册表，重新启动计算机。

```
REGEDIT4{HKEY_CURRENT_USER\Software\Microsfot\Windows\CurrentVersion\Policies\System}
"DiableRegistryTools"=dword:00000000
```

经过上面的几个步骤，我们对注册表进行了一些设置和改动，对 Windows 98 系统的设置进行修改之后，已经增强了它的安全性。可是，对于熟悉 Windows 98 系统安全漏洞的人来说，这些还远远不够。众所周知，所有与用户相关的文件均保存在 Windows 目录下的“Profiles”目录中，一个用户对应一个 Profiles 的下一级子目录，在这级子目录下又有多个下级子目录，下级子目录还有多级目录：Desktop(桌面设置的相关内容)、NetHoot(网络资源)、Program(“开始”菜单中的“程序”选项)、Recent(“开始”菜单中“文档”中的所有文件存放在内)、Start Menu(“开始”菜单中的相关项目)。其实，在 Windows 98 目录中，还可以找到以用户名(扩展名为.pwl)为文件的密码文件。如果将它删除，任何人都可以轻松地进入 Windows 98 系统，这就意味着，前面所做的防范工作全部都报废了。

前面我们提到，为了防止非法用户进入 Windows 98 系统，单击“取消”按钮也可以进入系统，在注册表中新加一个键值可以使非法用户无法登录。这里，还有另一种方法可以达到同样的目的。

在启动 Windows 98 时，按 F8 键，选择 SafeMode(安全模式)或者 Command Prompt only(命令提示模式，即我们常说的 DOS 模式)，用户就可以进入系统，然后删除系统目录下扩展名为.pwl 的文件，重新启动计算机，就可以随心所欲地操纵计算机了。

为了避免以上灾难的发生，有必要做好以下的防范工作。

首先，用记事本或者写字板打开 Windows 目录下的 System.ini 文件，打开“Password Lists”小节，如图 4-16 所示。如果已经进行了用户设置，就会在这里找到所有用户密码文件(*.pwl)及其保存的名称和路径。根据这些信息对密码文件名及其路径进行修改，也就等于隐藏了保存密码的文件。

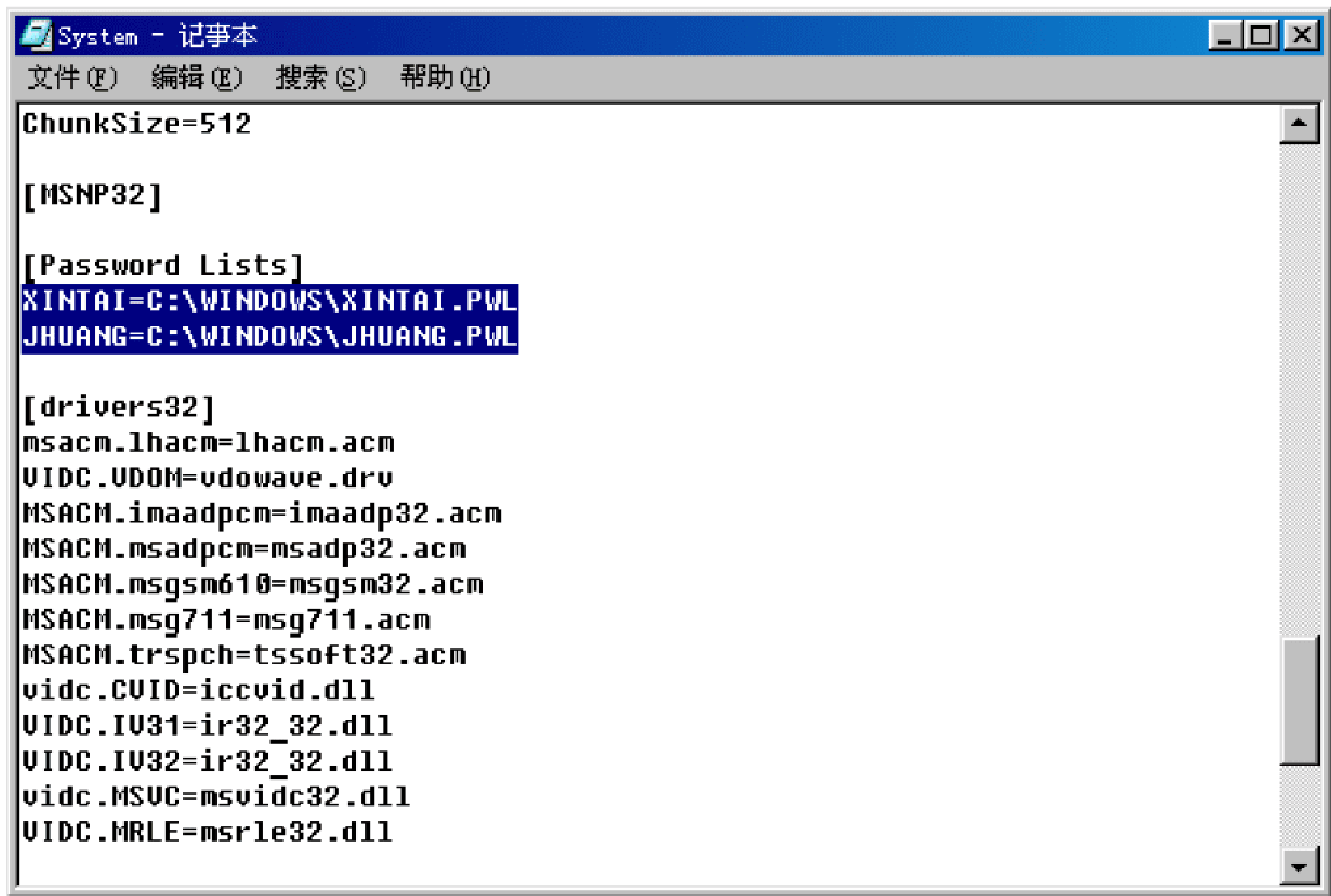


图 4-16　修改 System.ini 中关于用户密码的部分

其次，我们可以通过修改 MSDOS.SYS 文件来完成，打开 MSDOS 文件后，在该文件的[options]小节中加入以下几行。

- “BootMulti=0”：设置系统不能进行多重引导。
- “BootGUI=1”：在启动时候直接进入 Windows 98 图形用户界面。
- “BootDelay=0”：设置在启动时“Starting Windows 98…”信息停留的时间为 0 秒。
- “BootKeys=0”：设置在启动过程中的 F4、F5、F6、F8 功能键失效。

此外，为了防止用户从软盘或光盘启动计算机，在 CMOS 设置中，将启动顺序一项设置为 C only；然后给 CMOS 设置程序加一个密码。此时，Windows 98 系统或者说计算机已经有一个相对安全的运行环境了。

另外，对于禁止非法用户登录 Windows 98 系统，前文主要是通过修改注册表来实现的。在这里我们需要说明一下，在 Windows 98 系统启动光盘里有一个叫“策略编辑器”的应用程序，它也可以用来帮助用户完成禁止非法用户登录系统等许多关于安全防范方面的设置，但是这个程序不是默认安装的，用户如果需要，必须从 Windows 98 光盘上手动安装它。有兴趣的读者可以系统地学习“Windows 98 系统安全策略编辑器”的有关知识，在此就不再赘述。

2. Windows NT/2000/XP 的安全基础

Windows NT/2000/XP 操作系统不同于 Windows 95/98/ME 操作系统，在其设计的时候就已经把网络连接、安全和审核报告作为系统的核心功能之一，并在后期不断更新修正。可以说，Windows NT/2000/XP 操作系统就是建立在一套完整的网络安全机制之上的操作系统。Windows NT/2000/XP 操作系统的服务器对于网络而言，其安全性能远远超过了以往的 DOS、Windows 95/98/ME 等操作系统。尽管 Windows NT/2000/XP 操作系统的安全机制比较全面，但 Windows NT/2000/XP 操作系统在网络安全防范上仍没有做到尽善尽美，这是因为 Windows NT/2000/XP 操作系统本身也存在各种安全漏洞，并不解决安全问题。如果不了解这些安全漏洞，不采取相应的安全对策和防范措施，就会使计算机系统完全暴露在黑客的入侵范围之内，随时遭受攻击并被毁坏。因此，在使用 Windows NT/2000/XP 操作系统时，一定要了解系统

的安全模型、安全机制。加强安全管理，制订精细的安全策略，才能降低遭受威胁和黑客攻击的危险。本节将以 Windows 2000 操作系统为例介绍与其相关的内容。

1) Windows 2000 安全基础概念

在 Windows 2000 中用户可以在“活动目录用户和计算机”管理器中实现建立用户账号、计算机账号、组、安全策略等项。它可以用于建立或编辑网络中的用户、计算机、组、组织单位、域、域控制器以及发布网络共享资源等。活动目录用户和计算机管理器，是安装在域控制器上的目录管理工具，用户可以在 Windows 2000 Professional 中安装它的管理工具，以便利用客户机对活动目录进行远程管理。

(1) 用户账号

用户账号能够让用户以授权的身份登录到计算机和域中，访问其中的资源。用户账号也可以作为某些软件的服务账号。Windows 2000 在安装时候提供了以下两个预定义的用户账号。

● Administrator

Administrator 是系统管理员账号，拥有最高的权限，用户可以利用它来管理 Windows 2000 Server 的资源，但是 Administrator 并不是自动对 Server 中的所有目录和文件都拥有访问权限，管理员账号的名称可以更改，但是不可以删除。

● Guest

Guest 是为临时使用而设立的客户账号，它只有极少的权限，可以更改名称，也可以设置密码、修改头像等，但是不能删除，在默认状态下是不激活状态。

(2) 计算机账号

每一个运行 Windows 2000 和 Windows NT 的计算机，在加入到域的时候都需要一个计算机账号，就像用户账号一样，被用来验证和审核计算机的登录过程和访问域的资源。

(3) 组

组可以包含用户、联系人、计算机和其他组的 Active Directory 或本机对象。使用组可以做如下的工作。

● 管理用户和计算机对 Active Directory 对象及其属性、网络共享位置、文件、目录、打印机队列等共享资源的访问。
● 筛选组策略设置。
● 创建电子邮件(E-mail)通信组。

通常，组有两种类型：安全组和通信组。

安全组用于将用户、计算机和其他组收集到可管理的单位中。为资源(文件共享、打印机等)指派权限时，管理员应将权限指派给安全组而非个别用户。权限可以一次分配给这个组，而不是多次分配给单独的用户。使用组而不是单独的用户可以简化网络的维护和管理工作。

通信组只能用做电子邮件的通信组，不能用于筛选组策略管理，通信组无安全功能。

任何时候，组都可以从安全组转换为通信组，反之亦然，但仅仅限于域处于本机模式的情况，域处于混合模式时，不能转换为组。

(4) 域

域是网络对象的分组，例如，用户、组和计算机。域中所有的对象都存储在 Active Directory

下。Active Directory 可以常驻在某个域中的一个或多个域控制器下。每个域都是一个安全界限，这意味着安全策略和设置(例如系统管理权限、安全策略和访问控制表)不能跨越不同的域。特定域的系统管理员有权限设置仅属于该域的策略。由于每个域都是一个安全壁垒，因此不同的系统管理员可以在单位中创建和管理不同的域。理解域的关键是：安全策略可以贯穿整个域来实现。

- 为保证数据库的同步，包括安全信息的 Active Directory 会定期复制到域中每个域控制器。
- Active Directory 中的对象可以按组织单位的不同级别进行组织和管理。
- 可转移的信任关系可以建立在域树中的域之间。

Windows NT 限制了目录可以存储的用户账户的个数。因此，为了适应大环境的需要，创建和管理多个域并且每个域拥有各自独立的用户账户已经成为大势所趋。域通常使用以下两种类型进行组织：主域(存储用户和组的账户)和资源域(存储文件、打印机和应用程序服务等)。

这种多域的计算环境被称为主域模式。多主域模式意味着资源需要与所有的主域具有信任关系，这些信任关系允许主域的用户访问资源域中的资源。

(5) 身份验证

身份验证是系统安全性的一个基本方面，它负责确认试图登录域或访问网络资源的任何用户的身份。Windows 2000 身份验证允许对整个网络资源进行单独登记。采用单独登记的方法，用户可以使用单个密码或智能卡一次登录到域，然后通过身份验证向域中的所有计算机表明身份。具体包含以下几个步骤。

- 在 Windows 2000 计算环境中成功的用户身份验证包括两个独立的过程。
- 交互式登录向域账户或本地计算机确定用户的身份。
- 网络身份验证对该用户试图访问的任何网络服务确定用户身份。
- 在用户试图访问安全的 Web 服务器时使用。

(6) 授权

Windows 2000 的安全性建立在身份验证和授权之上。

管理员可以指派特定权利组账户或单个用户账户。

用户权利定义了本级别上的功能。虽然用户权利可以应用于单个的用户账户，但是最好是在组账户基础上管理。这样可以确保作为组成员登录的账户将自动继承该组的相关权限。通过对组而不是对单个用户指派用户权利，可以简化用户账户管理的任务。当组中的用户都需要相同的用户权利时，用户可以一次对该组指派用户权利，而不是重复地对每个单独的用户账户指派相同的用户权利。

对组指派的用户权利应用到该组的所有成员(在它们还是成员的时候)。如果用户是多个组的成员，则用户权利是累积的。这意味着一个用户允许拥有多组权利。指派给某个组的权利只有在特定登录权利的情况下才会与指派给其他组的权利发生冲突。然而，指派给某个组的用户权利通常不会与指派给其他组的权利冲突。要删除一个用户的权利，管理员只需简单地从组中删除该用户即可。在这种情况下，用户不再拥有指派给这个组的权利。

用户权利有两种类型：特权和登录权利。

- 特权：典型范例就是备份文件和目录的权利。
- 登录权利：典型范例就是登录本地系统的权利。

(7) 审核

安全审核是 Windows 2000 的一项功能，负责监视各种与安全性有关的事件。监视系统事件对于检测入侵者以及危及系统数据安全性的尝试是非常有帮助的。应该被审核的最普通的事件类型包括：

- 访问对象，例如文件和文件夹；
- 用户和组账户的管理；
- 用户登录以及从系统注销时。

除了审核与安全性有关的事件，Windows 2000 还生成安全日志，提供查看日志中所报告的安全事件的方法。

2) Windows 2000 用户账号的管理

(1) 添加用户账号

在 Windows 2000 Server 中，一个用户账号包含了用户的名称、密码、所属组、个人信息、通信方式等信息，在添加一个用户账户后，它被自动分配一个安全标识 SID，这个标识是唯一的，即使账号被删除，它的 SID 仍然保留。如果在域中再添加一个相同名称的账号，它将被分配一个新的 SID，在域中利用账号的 SID 来决定用户的权限。

添加用户账号的步骤如下。

① 双击“我的电脑”中的“控制面板”，在“控制面板”中双击“管理工具”，启动“Active Directory 用户和计算机管理器”，单击“user 容器”会看到在安装 Active Directory 时自动建立的用户账号。

② 选择“操作”→“新建”→“用户”，在“新建对象-用户”对话框中输入用户的姓名、登录名，其中第 2 个登录名是指当用户从运行 Windows NT/98 等老版本的操作系统的计算机登录网络所使用的用户名，单击“下一步”按钮，如图 4-17 所示。



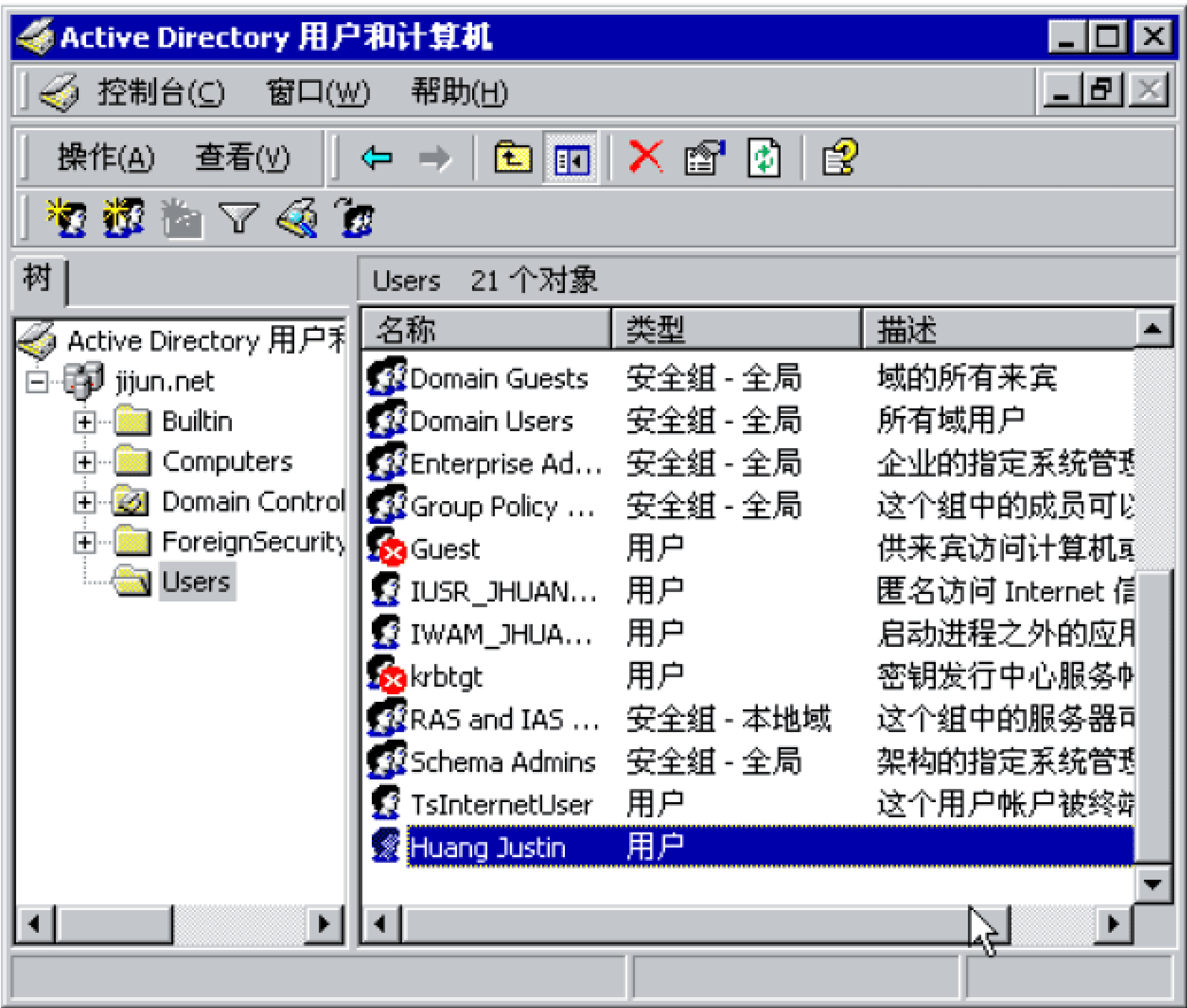
图 4-17　“新建对象-用户”对话框

③ 在“密码”对话框中输入密码或不填写密码同时选择“用户下次登录时须更改密码”复选框，以便让用户在第一次登录时可以修改密码，如图 4-18 所示。

④ 完成对话框的设置后，单击“完成”按钮，这时用户会在管理器中看到新添加的用户，如图 4-19 所示。



图 4-18　新建用户密码及相关选项图



4-19　新建用户在 Active Directory 用户容器里

(2) 管理用户账号

在用户属性对话框中的“常规”选项卡中，可以输入有关该用户的描述信息，诸如：办公室、电话、电子邮件地址及个人主页的网址；在“地址”选项卡中输入用户所在的地区及通信地址；在“电话/备注”选项卡中可以输入有关用户的家庭电话、寻呼机、移动电话、传真、IP 电话或者相关的备注信息。

① 设置用户登录时间

在“账户”选项卡中，单击“登录时间”按钮，出现如图 4-20 所示的对话框。



图 4-20　用户登录时间段设置

图中横轴的每个方块表示 1 小时，纵轴每个方块表示 1 天，右边蓝色的方块表示该时间段内允许用户使用，空白方块表示该时间段不允许用户使用。默认的是所有时间段都允许用户使用。系统管理员可以通过设置这里的信息，根据不同部门和用户的工作需要，设置不同的使用时间，以加强计算机系统的安全保障。对于非工作时间，没有特殊需要的用户和用户组，不允许使用特定的计算机资源，是一个简单有效的安全防范措施。

要禁止该用户在特定时间段登录的方法是：在该用户登录时段对话框中，选择需要禁止其登录的时间段，然后选择右边的“拒绝登录”单选按钮，之后确定退出即可。需要指出的是，如果该用户在允许其登录的时间段内登录到网络中，并且一直持续到超过了允许登录的时间，这种情况下，该用户可以继续连续使用，但是不允许建立新的连接，也就是说，该用户注销或退出后，系统将不允许其再次登录。

② 设置用户登录的计算机

在账户中，单击“登录到”按钮，出现如图 4-21 所示的对话框。

在默认情况下，用户可以从所有的客户机登录，也可以设置让用户在指定的某些工作站登录，而不能在其他的工作站登录。设置时输入计算机的名称(NetBIOS 名)，然后单击“添加”按钮即可。需要注意的是，这些设置对于非 Windows NT/2000 的工作站是无效的，因此用户可以不受这个设置限制，从任何一台 DOS、Windows 客户机登录到网络中。



图 4-21　“登录工作站”对话框

③ 设置账户的有效期限

在账户的下方，用户可以选择账户的使用期限，默认情况下账户是永久有效的，但对于临时工作人员来说，设置账户的有效期限是非常必要的。在有效期过后，该账户会被自动标记为失效，默认的期限是一个月，管理员可以通过手动设置修改这个期限的长短。

3) Windows 2000 组的管理

用户可以利用将用户加入到组中的方式，简化网络的管理工作。当用户对组设置了权限，该组的所有用户就具有了赋予的权限，大大简化管理员对单个用户重复设置同样权限的操作，提高工作效率。

(1) 添加组

具体步骤如下。

① 双击“我的电脑”中的“控制面板”，在“控制面板”中双击“管理工具”，打开“Active Directory 用户和计算机管理器”。

② 在控制台树中，双击域节点。

③ 右击要添加组的文件夹，指向“新建”，然后单击“组”。

④ 输入新组的名称，在默认情况下，用户输入的名称还将作为新组的 Windows 2000 以前的版本名称，如图 4-22 所示。



图 4-22　“新建对象-组”对话框

⑤ 单击所需的“组作用域”。

⑥ 单击所需的“组类型”。

注意：如果用户目前创建的组所属的域处于混合模式，只能选择具有“本地域”或“全局作用域”的安全组。

(2) 指定用户隶属的组

具体步骤如下：

在组属性对话框中打开“成员属于”选项卡，如图 4-23 所示，可以查看到当前用户隶属的组，如果要将用户添加到其他的组，可以单击“添加”按钮，出现如图 4-24 所示的对话框，在上方的窗体中选择需要添加的组(可以按住 Shift 或者 Ctrl 键，利用鼠标进行多选)，然后单击“添加”按钮，所选的组会出现在下方的窗体中，单击“确定”按钮即可。

如果需要将用户从他所属的组中删除，可以在成员“隶属于”窗体中选择该组，单击“删除”按钮。注意：用户账号至少隶属于一个组，该组被称为主要组，这个主要组必须是一个全局组且它不可被删除。



图 4-23　指定用户属性的对话框

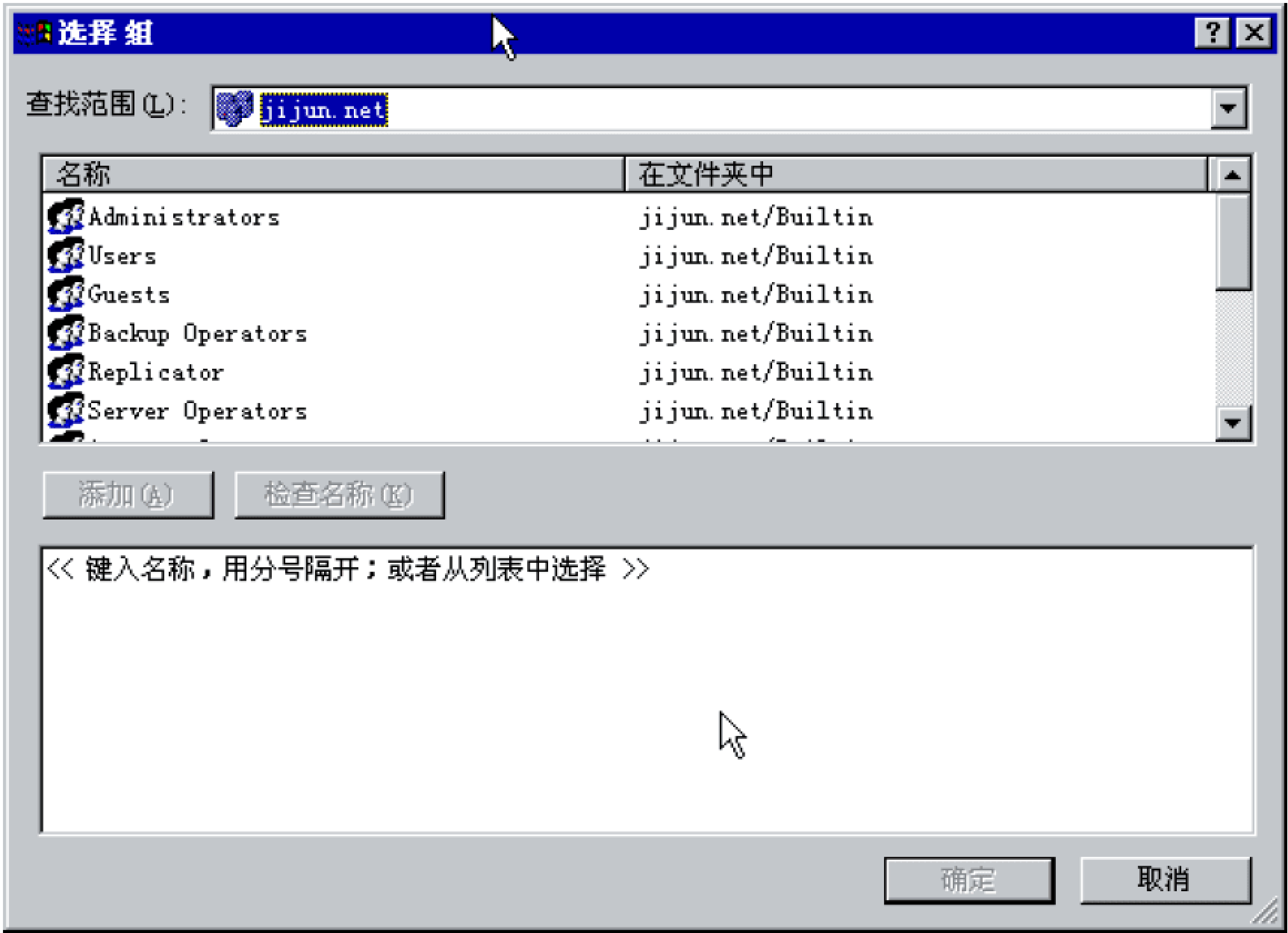


图 4-24　“选择组”对话框

(3) 管理组

将组转换为另一种组类型的步骤如下。

① 双击“我的电脑”中的“控制面板”，在“控制面板”中双击“管理工具”，打开“Active Directory 用户和计算机管理器”。

② 在控制台树中，双击域节点。

③ 单击包含该组的文件夹。

④ 在详细信息窗中，右击组，然后选择“属性”命令。

⑤ 在“常规”选项卡的“组类型”中，选择“分布式”或者“安全式”。

更改组作用域的具体步骤如下。

① 双击“我的电脑”中的“控制面板”，在“控制面板”中双击“管理工具”，打开“Active Directory 用户和计算机管理器”。

② 在控制台树中，双击域节点。

③ 单击包含该组的文件夹。

④ 在详细信息窗中，右击组，然后选择“属性”命令。

⑤ 在“常规”选项卡的“组作用”中，选择“本地域”、“全局”或“通用”。

删除组的步骤如下。

① 双击“我的电脑”中的“控制面板”，在“控制面板”中双击“管理工具”，打开“Active Directory 用户和计算机管理器”。

② 在控制台树中，双击域节点。

③ 单击包含该组的文件夹。

④ 在详细信息窗中，右击组，然后选择“删除”命令。

4.1.3　Windows 操作系统的基本安全设置

安全设置定义了系统的安全相关操作。通过使用 Active Directory 中的组策略对象，系统

管理员可以集中应用保护企业系统所要求的安全级别。

安全设置包括安全策略(账户和本地策略)、访问控制(服务、文件、日志、注册表)、事件日志、组成员(受限的组)、网际协议(IP)的安全策略和公钥管理。

安全模板是安全设置的物理表现，一组安全设置应该存储于一个文件中。Windows 2000 包括一组以计算机的角色为基础的安全模板，从低安全域客户端的安全设置到非常安全的域控制器。这些模板可用于创建自定义安全模板，修改模板或者作为自定义安全模板的基础。

安全设置工具是管理员用来进行安全设置的。

- 管理员可使用安全模板管理单元来定义和使用安全模板。
- 管理员可使用安全设置和分析管理单元设置分析本地的安全性。
- 管理员可使用组策略管理单元设置 Active Directory 中的安全性。

4.2　Windows NT/2000 安全

根据《可信计算机系统评价准则》(TCSEC，又称橘皮书，详细内容参见第 2 章的相关内容)的安全等级划分，Windows NT/2000 操作系统具有 C2 级安全标准，并且支持以下几种安全协议。

1. Windows NT Lan Manager(NTLM)验证协议

NTLM 协议是 Windows NT 4.0 操作系统中网络验证的默认协议。NTLM 验证的缺点是没有连续性，速度较慢，不能跨网络验证，不允许客户验证服务器身份，或者一个服务器验证另一个服务器的身份。NTLM 验证用于传递网络身份验证、远程文件访问，以及与 Windows NT 早期版本建立的已验证远程过程调用(RPC)连接。

2. Kerberos V5 验证协议

Kerberos V5 协议是 Windows 2000 中网络验证的默认协议。Kerberos 协议比 NTLM 更加灵活有效，并且更加安全。Kerberos 身份验证协议是一个成熟的行业标准，在 Windows 网络身份验证方面具有很多优势。使用 Kerberos 验证，服务器不再需要连接到域控制器。Kerberos 验证还支持客户机和服务器的相互身份验证。

3. DPA 分布式密码验证协议

这是某些规模较大的 Internet 成员组织，如 Microsoft MSN 或 CompuServe，所使用的共享秘密身份验证协议。此身份验证协议是 Microsoft 商业 Internet 系统(MCIS)服务的一部分，其用户只需一套账号和密码，即可访问 Internet 会员组织内的所有站点。

4. 基于公共密钥的协议

在此协议中，每个参与者都有一对密钥，可以分别指定为公钥和私钥，一个密钥加密的消息只有另一个密钥才能解密，而从一个密钥推断不出另一个。公钥可以用来加密和验证签名；私钥可以用来解密和数字签名。每个人都可以公开自己的公钥，以供他人向自己传输信

息时加密使用。只有拥有密钥的本人才能解密，保证了传输过程中的保密性、安全性。

4.2.1 Windows NT/2000 文件系统

NTFS 文件系统是 Microsoft 公司开发的一套具有优异性能的文件系统，相比早期的 FAT 和 FAT32，功能要强大很多，它提供了高性能、安全性和可靠性，这些在所有 FAT 版本中都没有实现的高级功能，是一种高级文件系统。NTFS 可以通过使用标准的事务处理记录和还原技术来保证卷的一致性；在 Windows 2000 和 Windows XP 中，NTFS 还可以提供诸如文件和文件夹权限、加密、磁盘配额、压缩等高级功能；同时它还包括提供了 Active Directory 所需的功能以及其他重要安全性能，只要通过选择 NTFS 作为文件系统才能使用诸如 Active Directory 和基于域的其他重要安全性功能；要维护文件和文件夹访问控制并支持有限个账户，必须使用 NTFS，而如果使用 FAT32，所有用户都将具有访问权，来访问您的硬盘驱动器上的所有文件，而不考虑其账户类型，例如管理员、有限制的或者标准的；此外，NTFS 是一种适合处理大磁盘的文件系统。表 4-1 比较了 FAT、FAT32、NTFS 支持的磁盘和文件大小。

表 4-1　NTFS、FAT 和 FAT32 的比较

NTFS	FAT	FAT32
推荐最小容量为 10MB，也可使用大于 2TB 的卷。无法在软盘使用	容量可以从软件大小到 4GB。不支持域	容量从 512MB 到 2TB。在 Windows XP 中，只能格式化最多达 32GB 的 FAT32 卷。不支持域
文件大小只受卷的容量限制	文件最大为 2GB	最大文件长度为 4GB

文件系统的安全性方面，Windows NT 和 Windows 2000 都支持保证文件和文件夹安全性的访问控制列表(Access Control List，ACL)。

用于控制账户访问文件的 ACL，如表 4-2 所示。

表 4-2　文件控制列表

权　限	说　明
无	用户不可访问文件
读取	用户可以查看文件中的数据
写入	用户可以更改文件中的数据
执行	用户可以运行程序文件
删除	用户可以删除文件
更改权限	用户可以更改文件权限
获取所有权	用户可以取得文件所有权，所有者同时拥有该文件的其他访问权限

用于控制账户访问文件夹的 ACL 如表 4-3 所示。

表 4-3　文件夹访问的控制列表 ACL

文件夹 ACL	说　　明
无	用户不可访问文件夹
读取	用户可以查看文件夹中的文件名和子文件夹名称
写入	用户可以向文件夹添加文件和子文件夹
执行	用户可以更改文件夹的属性
删除	用户可以删除文件夹或子文件夹
更改权限	用户可以更改文件夹权限
获取所有权	用户可以取得文件夹所有权，所有者同时拥有该文件夹的其他访问权限

文件夹权限包括：完全控制、修改、读取和执行，列出文件夹目录，读取和写入。这些权限的每一项具体功能都是由表 4-4 列出和定义的特殊权限所构成的逻辑组成。

表 4-4　文件夹权限及其定义说明

访 问 权 限	说　　明
通过文件夹执行文件	对于文件夹：允许或拒绝通过文件夹访问某些文件或文件夹，即使用户没有所通过的文件夹(只适用于文件夹)的访问权限。只有当“组策略”管理单元中没有授予组或用户“忽略通过检查”用户权限时，“通过文件夹”才起作用。默认情况下，授予 Everyone 组“忽略通过检查”用户权限 对于文件：“执行文件”允许或拒绝运行程序文件(仅适用于文件) 设置文件夹的“通过文件夹”权限不会自动设置该文件夹中所有文件的“执行文件”权限
列出文件夹、读取数据	“列出文件夹”允许或拒绝用户可以查看文件夹中的文件名和子文件夹名称。“列出文件夹”只影响该文件夹的内容，不影响是否列出正在设置其权限的文件夹。它只适用于文件夹 “读取数据”允许或拒绝查看文件(只适用于文件)中的数据
读取属性	允许或拒绝查看文件或文件夹的属性，例如只读和隐藏。属性由 NTFS 定义
读取扩展属性	允许或拒绝查看文件或文件夹的扩展属性，扩展属性由程序定义，可能因程序而异
创建文件，写入数据	“创建文件”允许或拒绝在文件夹(仅适用于文件夹)内创建文件 “写入数据”允许或拒绝更改文件和覆盖已有的内容(适用于文件)
更改权限	用户可以更改文件夹权限
创建文件夹，添加数据	“创建文件”允许或拒绝在文件夹(仅适用于文件夹)内创建文件 “添加数据”允许或拒绝更改文件的末尾，不限制更改、删除或覆盖已有的数据(适用于文件)
写入属性	允许或拒绝更改文件或文件夹的属性，例如只读和隐藏。属性由 NTFS 定义 “写入属性”权限没有表示可以创建或者删除文件或文件夹，它只包括更改文件或文件夹属性的权限。要允许或拒绝创建或删除操作，请参阅“创建文件，写入数据”、“创建文件夹，追加数据”、“删除文件夹和文件”以及“删除”等相关权限内容

(续表)

访 问 权 限	说　　明
写入扩展属性	允许或拒绝更改文件或文件夹的扩展属性。扩展属性由程序定义，可能因程序不同而有所差异 “写入扩展属性”权限不表示可以创建或者删除文件或文件夹，它只包括更改文件或文件夹属性的权限。要允许或拒绝创建或删除操作，请参阅“创建文件，写入数据”、“创建文件夹，追加数据”、“删除子文件夹和文件”以及“删除”等相关权限内容
删除子文件夹和文件	允许或拒绝删除子文件夹和文件，即使尚未授予对子文件夹或文件的“删除”权限(适用于文件夹)
删除	允许或拒绝删除文件或文件夹。如果没有对文件或文件夹的“删除”权限，但是在父文件夹中已被授予“删除子文件夹和文件”，那么仍然可以删除
读取权限	允许或拒绝读取文件或文件夹权限，例如完全控制、读取、写入
更改权限	允许或拒绝更改文件或文件夹权限，例如完全控制、读取、写入
取得所有权	允许或拒绝取得文件或文件夹的所有权。文件或文件夹的所有者始终可以更改其权限，无论是否存在任何保护该文件或文件夹的权限
同步	允许或拒绝不同的线程在句柄上等待文件或文件夹，并与另一个可能向它发信号的线程同步。该权限只应用于多线程、多进程的程序

表 4-5 为对文件和文件夹权限的描述，包括：完全控制、修改、读取和执行、列出文件夹目录、读取和写入。需要注意的是，无论有什么权限保护文件，被准许对文件夹执行“完全控制”的组或用户都可以删除该文件夹内的任何文件。

表 4-5　文件和文件夹权限

特 殊 权 限	完 全 控 制	修　改	读取和执行	列 出 目 录	读　取	写　入
通过文件夹执行文件	×	×	×	×		
列出文件夹读取数据	×	×	×	×	×	
读取属性	×	×	×	×	×	
读取扩展属性	×	×	×	×	×	
创建文件写入数据	×	×				×
创建文件夹添加数据	×	×				×
写入属性	×	×				×
写入扩展属性	×	×				×
删除文件夹和文件	×					
删除	×	×				
读取权限	×	×	×	×	×	×
更改权限	×					
取得所有权	×					
同步	×	×	×	×	×	×

4.2.2　Windows NT 安全漏洞及解决方案

Windows NT 越来越受到广大计算机用户的欢迎。Internet 上采用 NT 平台作为服务器的站点越来越多，同时，众多的企业已经采用 NT 平台作为企业内部计算和网络 Intranet 的解决方案。Windows NT 系统上的重大安全漏洞，集中体现在两个方面：NT 服务器和工作站的安全漏洞；关于浏览器和 NT 系统的严重安全漏洞。

有一些知名的网站，如 addoil.net，专门公布操作系统的安全漏洞，在 addoil.net 中就描述了几十个关于 Windows NT 系统的安全漏洞名称、解释以及降低风险的一些建议。目前，时不时都有不断公布的漏洞被发现的报导，以及微软公司发布的漏洞修补补丁。因此，对于 Windows 用户来说，定时定期下载安装系统漏洞的补丁，是一个保障系统安全的好习惯。

其实，众所周知的事实是，养成定时安装漏洞补丁的习惯，不是一个根治问题的办法，更加有效的解决方案是：建设一个强大的防火墙，精心配置它，只授权给可信赖的主机通过防火墙访问外部网络资源。

4.2.3　Windows 2000 分布式安全协议

在 Windows NT 4.0 中，主要的分布式安全协议是 NTLM(Windows NT LAN Manager，Windwos NT 操作系统的安全保护协议)。而在 Windows 2000 中，微软采用了一个新的安全系统。在这个新的系统中，Kerberos 是默认的分布式安全协议。当然，Windows 2000 秉承了一贯的向下兼容的做法，仍然支持 NTLM 以及 SSL 协议。

1. Kerberos

Kerberos 是在 20 世纪 80 年代早期由著名的麻省理工学院 MIT 创建的，Windows 2000 实现的是标准的 Kerberos 协议。在 Windows 2000 中 Kerberos 是以安全服务提供者(Security Service Provider，SSP)的方式通过安全服务提供者接口(Security Service Provider Interface，SSPI)来实现的。应用程序可以直接通过 SSPI 来获取 Kerberos 的服务。实际上，SSL 的大多数应用程序都不会直接利用 SSPI，不过，有一些应用程序是直接调用 SSPI 的，一个分布式的 COM、DCOM 或者 COM+利用 DCOM 提供的安全接口。实际上，DCOM 是利用认证过的远程调用 RPC 接口，而该接口是直接调用 SSPI 的。除此之外，大多数协议把 SSPI 的实现细节封装起来，因此用户没有必要担心实现分布式安全协议的具体实现细节。

Kerberos SSP 能够提供三种安全性服务：认证(进行身份验证)、数据完整性(保证数据在传输过程中不被篡改)、数据保密性(保证数据在传输过程中不被获取)。Kerberos 通过加密来实现这些服务。Windows 2000 提供公钥和私钥加密，在私钥加密中，加密和解密的密钥是相同的。Kerberos 不需要用户(一个安全实体)用一个特别的加密密钥，而只使用一个一般的密码。在 Windows 2000 中，密码不会直接用来加密用户和服务器之间传送的数据。事实上，那些基于密码的密钥仅在登录时有效，其他用来加密在网络上传送数据的密钥，都是动态产生的。因此，准确的解释是，用户用来登录的密钥是用户密码的散列值。由于散列算法是单向的，因此，给定一个密钥的散列值是无法获得密码的。在 Windows 2000 中，每个用户都拥有密码，而访问服务器都会要求认证用户的密码。域中任何一个拥有密码的实体成为一个

安全实体。运行在域控制器上的 Kerberos 服务器本身称为密钥分发中心(KDC)。域控制器拥有访问这个域内每个安全实体密码的散列值的权限(这些信息是放在实体活动目录中的，也放在域控制器上)。通常明文的密码并不放在这个目录下，仅仅是密码的 HASH 值存放在这里。不过，为了保持密码的同步，一个管理员可以同时在这个目录下存放用户的明文密码和散列值。

Kerberos 协议允许对加密算法进行协商，大多数 Kerberos 通过 DES 算法来实现，考虑到兼容性的问题，Windows 2000 采用的是 RC4 的算法，RC4 算法具有比 DES 算法更快、更安全的优点。

2. 认证

当用户要向服务器验证自己的身份的时候，这个用户必须向服务器提供一个适当的 Ticket(门票)，类似去电影院看电影需要门票一样，身份认证需要每个进门的人出示一张有效门票方可放行。每个 Ticket 允许一个特定的用户向一个特定的服务器证实自己的身份。Ticket 包括加密部分和未加密部分，其中，未加密部分通常包括：

- 这个 Ticket 是由哪个 Windows 2000 的域发出来；
- 该 Ticket 定义的实体名字。

加密部分一般包括：

- 各种标志；
- 一个加密密钥，通常是一个会话密钥，用来加密该 Ticket 中指明的用户和该 Ticket 的目的服务器之间的数据；
- 加密后的用户实体名字和域名；
- Ticket 的有效生存周期；
- 用户系统的 IP 地址；
- 用户认证数据，通常是服务器用来确认该用户的存取权限；
- 其他部分。

所有这些部分都被服务器方的密钥加密过，无论是用户还是攻击者都无法修改或获取 Ticket 的加密部分，原因是他们没有服务器方合法的密钥。每个 Ticket 都有其生存周期，也就是在更新一个 Ticket 之前的这段间隔时间内，攻击者只有有限的时间来破译之前的 Ticket。这就使得非法入侵者的攻击更加困难，而且一个被盗用的 Ticket 也只能使用到它的终止时间，时间到期就要重新破译新的 Ticket。在用户登录以后，Windows 2000 会自动更新用户的 Ticket。

当一个用户要向一个服务器证实自己的身份时，必须获得该服务器认可的一张 Ticket，也就是门票。而 Kerberos 就是用来获取和使用 Ticket 的协议，通俗的解释就是，沟通的双方必须使用一种双方都能理解的语言，以及双方都认可的方式进行沟通，进而验证对方身份是否合法。在进一步说明协议的工作原理之前，我们只简单介绍 Kerberos 的基本原理，详细的协议说明在后续的章节里会有专门的介绍。

3. 数据的完整性和保密性

以上介绍的是 Kerberos 提供的一个安全性服务——身份认证。需要指出的是，Kerberos

也能提供数据的完整性和保密性保障。

完整性：为了保证数据在传输的过程中不被篡改，发送方的 Kerberos SSP 会对它发送的每个报文计算校验值，并将该值和报文一起发送。这个校验值是数据的函数值，因此当数据发生变动时，它的校验值也会相应地发生改动。不过，如果仅仅是提供一个报文和一个校验值，是无法防止攻击者篡改数据的，因为攻击者不仅利用消息本身来计算校验值，还包括其他的信息。在 Windows 2000 中，Kerberos 用的校验值算法称为 HMAC(基于散列的消息认证码)，这个校验值是用 RC4 来加密的，尽管攻击者可以创建一个校验值，但是由于他不知道密钥，因此，报文的接受者可以辨别数据的真伪，从而达到验证的目的。

保密性：因为客户和服务器共享一个密钥 K(c，s)，每一端的 Kerberos SSP 都用这个密钥进行加密，由于攻击者无法更改网络上加密的数据，因此数据的保密性蕴含着数据的完整性，两者相辅相成。

4. 代理

假设用户已经向一个服务器 S 进行了身份验证并且试图询问服务器本地上的数据，例如一个文件。在这种情况下，由 Windows 2000 来实现基于文件 ACL 的访问控制。但是如果要访问的数据不在本地，该如何解决呢？

举个简单的例子，用户向远程的服务器发出请求，这时，服务器 S 就必须向另一个服务器 T 发出请求，虽然服务器 T 的直接用户是服务器 S，但实际访问的是用户，而不是服务器 S。为了安全稳定地工作，用户必须向服务器 S 说明自己的身份，并且允许服务器 S 代表自己向远程服务器发出请求。

Kerberos 可以通过代理来实现。如果一个客户应用程序请求服务，一个用户的 Ticket 和它的相关密钥被发送到另一个服务器上，像所有的 Ticket 一样，都是被加密过的，但是为了确保在传输过程中密钥不被非法攻击者截获，这个密钥用客户和服务器 S 共享的会话密钥进行加密。

Kerberos 同时也允许在不同的域的客户和服务器之间进行认证，不论用户想访问哪个服务器，都必须事先获得一个到该服务器的 Ticket。

Windows 2000 中，Kerberos 支持传递的信任关系，也就是说，如果一个 Windows 2000 的域信任第二个域，而第二个域又信任第三个域，根据传递性，第一个域会自动信任第三个域。在 Windows 2000 中，任一个域树或森林中，域之间的信任关系总是双向的，这种传递性使得每个域仅需要知道在域层次中它上面的和下面的域的密码。

4.3　UNIX 系统安全基础

UNIX 操作系统也具有 C2 级的安全级别，是一个相对安全、稳定的操作系统。UNIX 操作系统的安全焦点是文件许可权，其中包括：读许可权、写许可权以及执行许可权。

读许可权表明允许读取某个文件或目录。例如用 cat 命令读具有读许可权的文件的内容，也可以拷贝这类文件，或列出具有读许可权的目录。

写许可权标明允许修改写入一个文件。但是必须注意的是，可以修改一个文件的权限，并不代表一定可以删除该文件或对该文件重新命名，只有对该文件所在的目录有写许可权才能进行这两个操作。当用户具有对一个目录的写许可权后，就可以在该目录中建立一个新的文件，或者删除、重命名该目录中的文件。

执行许可权表明允许用户执行该文件。对文件而言，表明拥有此权限者可以执行该文件。如果该文件不是可执行的文件，执行许可权的授权是没有实际意义的。以目录而言，拥有对目录的执行许可权，是指允许打开该目录中的文件，并且可以用 cd 命令进入该目录。

4.3.1　UNIX 操作系统安全基础

1. 口令安全

UNIX 系统中的/etc/passwd 文件含有全部系统需要的关于每个用户的密码信息，加密后的口令也可能存于/etc/shadow 中。

/etc/passwd 中包含有用户的登录名、经过加密的口令、用户名、用户组名、用户注释、用户主目录和所有用户的 shell 程序。其中用户号 UID 和用户组号 GID 用于 UNIX 系统唯一标识用户和用户组以及用户的访问权限。

/etc/passwd 中存放的加密的口令，用于在用户登录时候经计算机校验，符合则允许登录，否则将拒绝用户登录。用户可以用 password 命令自行修改自己的口令，而不能直接修改/etc/passwd 中的口令部分的信息。

一个保密性好的口令，至少应当包含 6 个字符长度，一般建议不要取个人信息，如生日、名字、反向拼写的字母或者有些人能记住的有特殊意义的符号和数字，普通的英语单词也不建议采用，因为可以用字典攻击法穷举所有的单词进行破解。口令中最好有一些非字符类的，例如，数字、标点符号、控制字符等。最重要的，也是必须要记住的一点，是密码要容易被用户自己记忆，不要写在纸上或者计算机的文件里，以免被他人非法访问之后窃取。建议将两个不相关的词用一个数字或者控制字符连接起来，截断为 8 个字符作为口令。当然，如果用户能很容易地记住 8 个杂乱无章的乱码则最好。

不应使用同一个口令在不同的机器中登录，特别是在不同安全级别的计算机上使用同一个口令，很容易使整体的系统受到威胁。用户应定期修改口令，至少应 6 个月更改一次，系统管理员可以强制要求用户定期修改自己的口令。为了防止眼明手快的人窃取口令，在输入口令时候应该确认无外人在场。

2. 文件许可权

文件属性决定了文件被访问的权限，也就是规定了什么用户能存取或者执行该文件。用 ls –l 可以列出详细的文件目录及其权限信息，通常我们会看到文件属性部分有如下的信息。

```
-rwxrwxrwx
```

具体含义如下。

-：表示文件的类型。

第一个 rwx：表示文件属主的访问权限。

第二个 rwx：表示文件同组用户的访问权限。

第三个 rwx：表示其他用户的访问权限。

若某种许可被限制，则相应的字母换为-。

在许可权限的执行许可位置上，可能是其他字母：s、S、t、T 等。s 和 S 可能出现在所有者和同组用户许可的位置上，与特殊的许可有关；t 和 T 可能出现在其他用户的许可模式位置上，与“粘贴位”有关，而与安全无关。小写的字母(x，s，t)表示执行许可为允许，负号或者大写字母(-，S，T)表示执行许可为不允许。

改变许可方式的命令是 chmod 命令，并以新的许可方式和该文件名为参数，许可方式以 3 位 8 进制数为表现形式，例如 r 是 4，w 是 2，x 是 1，如果要给一个文件设置属性为 rwxr-xr-，对应的数值就是 754。

chmod 命令也有其他方式的参数，可以直接对某组参数进行修改。在此我们不再详细介绍，需要了解的读者请自行参阅 UNIX 系统相关的书籍和手册。

文件许可权可以用于防止误操作，如误删了或者写入了一个重要文件，即使是属主本人，也可以防止这样的低级错误造成的损失。

改变文件的属主和组，可以用 chown 和 chgrp 命令，但是修改后原属主和组员就无法修改回来了。

3. 目录许可

前面介绍的是文件许可，现在来介绍 UNIX 系统下的目录许可。其实，在 UNIX 系统中，目录也被看成是一个文件，不同的是它具有与文件不同的标识位。在用 ls –l 列出文件清单的时候，目录文件的属性前面带有一个 d 字母，表明该文件是一个目录。目录许可也类似于文件许可，用 ls 列目录要有读许可权，在目录中新建或者删除文件要有写权限，进入目录或者将该目录作为路径常量时，必须有执行许可权，因此要使用任一个文件，必须有该文件及找到该文件的路径上所有目录常量的相应许可权。当打开一个文件时，文件的许可才开始起作用，而 rm 和 mv 只要有目录的搜索和写许可，不需要文件的许可，这一点在使用过程中需要注意。

4. umask 命令

umask 设置用户文件和目录的文件创建默认屏蔽值，如果将此命令放入.profile 文件，就可以控制该用户后续所建立的文件的存取许可。umask 命令与 chmod 命令的作用正好相反，它告诉系统在创建文件时不给予什么存取许可。

5. 设置用户 ID 和同组用户 ID 许可

针对某个目标文件可分别设置 SUID(Set User ID，设置用户 ID)、SGID(Set Grouf ID，设置组 ID)权限。当一个进程执行时就赋予 4 个编号，以标识该进程隶属于谁，这 4 个编号分别为实际和有效的 UID、实际和有效的 GID。有效的 UID 和 GID 一般和实际的 UID 和 GID 相同，有效的 UID 和 GID 用于系统确定该进程对于文件的存取许可。而设置可执行文件的

SUID 许可将改变上述的情况，当设置了 SUID 时，进程的有效 UID 为该可执行文件的所有者的有效 UID，而不是执行该程序的用户的有效 UID，因此，由该程序创建的都有与该程序所有者相同的存取许可权。这样，程序的所有者将可以通过程序的控制在有限的范围内向用户发表不允许被公众访问的信息。

同样，SGID 是设置有效的 GID。

一般用 chmodu+s 文件名和 chmodu –s 文件名来设置和取消 SUID 设置。用 chmod g+s 文件名和 chmod g-s 文件名来设置和取消 SGID 设置。

当对文件设置了 SUID 和 SGID 后，chown 和 chgrp 命令将全部取消这些许可。

6. cp、mv、ln 和 cpio 命令

1) cp 拷贝文件

拷贝文件时，如果目的文件不存在，则将同时拷贝源文件的存取许可，包括 SUID 和 SGID 许可。新拷贝的文件属于拷贝的用户所有，因此拷贝他人的文件时要特别小心，不要让其他用户的 SUID 程序破坏自己的文件安全。

2) mv 移动文件

移动文件时，新的文件存取许可和源文件相同，mv 仅改变文件的名字。只要用户有目录的写和搜索许可权，就可以移走该目录中某人的 SUID 程序并且不改变其存取许可。如果目录许可设置不正确，则用户的 SUID 程序可能被移到一个他不能修改和删除的目录中去，并出现安全漏洞。

3) ln 建立一个链

为现有的文件建立一个链，也就是建立一个引用同一个文件的新名字。如果目的文件已经存在，则该文件将被删除而被新的链取而代之，或存在的目的文件不允许用户写入，则请求用户确认是否删除该文件，只允许在同一个文件系统内建立链。如果 SUID 文件已有多个链，改变其存取的许可方式，将同时修改所有链的存取许可；也可以用 chmod000 文件名，这样不仅取消了文件的 SUIDhe SGID 许可，也取消了文件的全部的链。要想找到什么文件与自己的 SUID 程序建立了链，不要立刻删除该程序，系统管理员可以用 ncheck 命令找到该程序的链。

4) cpio 拷贝目录结构

cpio 命令用于将目录结构拷贝到一个普通文件中，而后再用 cpio 命令将该普通文件转成目录结构。用-i 选项时，cpio 从标准输入设备读文件和目录列表，并将其内容按档案格式拷贝到标准输出设备；使用-o 选项时，从标准输入设备读取事先建立好的档案，重建目录结构。cpio 命令常用以下命令拷贝一完整的目录系统档案。

find from dir-print|cpio-o>archive

根据档案文件重建一个目录结构的命令如下。

cpio –id < archive

cpio 的安全约定如下。

- 档案文件存放着每个文件的信息。这些信息包括文件所有者、组用户、最后修改时间、最后存取时间、文件存取许可方式。

- 现存文件与 cpio 档案中的文件同名。如果现存文件比档案中的文件更新，这些文件将不会被重写。
- 如果拷贝时用修改选项 U，则同名的文件将被重写。有一个问题值得关注，如果被重写的文件原先与另一个文件建立了链，文件被重写后，链没有断开。也就是说，该文件的链将被保留下来，因此该文件的所有链实际指向从档案中提取出来的文件，运行 cpio 无条件重写现存文件以及改变链的指向。
- cpio 档案中包含的全路径名或父目录名给文件。即可以使用绝对路径或者相对路径来对目标档案进行操作，这是一种相对比较灵活的处理方式。举例说明：

```
find . -print -depth | cpio -ov >tree.cpio
```

该命令将把当前目录及子目录下的所有文件全部打包输出给文件 tree.cpio。

7. su 和 newgrp 命令

1) su 命令

su 命令可以不必注销当前用户而将另一个用户又登录进入系统，作为另一个用户进行工作。它将启动一个新的 shell，将有效和实际的 UID 和 GID 设置给另一个用户。

2) newgrp 命令

与 su 相似，用于修改当天所处的组名。

8. 文件加密

crypt 命令可以提供给用户加密文件的功能。使用一个关键词将标准输入的信息编码为不可读的杂乱字符串，送到标准输出设备。再次使用此命令，用同一个关键词作用于加密后的文件，可以恢复文件的内容。一般来说，在文件加密后，应删除原始文件，只留下加密后的版本，切记不能忘记加密的关键词。

在 vi 中一般都有加密功能，用 vi –x 参数可以编辑加密后的文件。关于加密关键词的选取，通常与口令的选取原则类似。

由于 crypt 程序可能被做成特洛伊木马，因此不宜用口令作为关键词。最好在加密前用 pack 或者 compress 命令对该文件进行压缩后再加密。

9. 其他安全问题

1) 用户.profile 文件

由于用户的 HOME 目录下的.profile 文件在用户登录时就被执行，如果该文件对于其他人也是可写的，那么系统的任何用户都可以修改它，使其按照自己的要求去工作，这样可能导致其他用户具有该用户相同的权限。

2) ls -a 命令

此命令用于列出当前目录中的全部文件，包括文件名以“.”开头的文件，查看所有的文件的存取许可方式和文件所有者，任何不属于自己但存在于自己的目录中的文件都有可能是非法入侵的怀疑对象和病毒的衍生物。

3) . exrc 文件

为编辑程序的初始化文件，使用编辑文件后，首先查找$HOME/.exrc 文件和./.exrc 文件，如果该文件在$HOME 目录中找到，就可以像.profile 一样控制它的存取方式。如果在一个自己不能控制的目录中运行编辑程序，则可以运行其他人的.exrc 文件，或许该.exrc 文件存放在那里是为了威胁他人的文件安全。为了保证所编辑文件的安全，最好不要在不属于自己或其他人可写的目录中运行任何编辑程序。

4) 暂存文件和目录

在 UNIX 系统中，临时目录一般为/tmp 和/usr/tmp，通常，程序员和许多系统命令都会用到它们，如果用这些目录存放暂时文件，别的用户则可能会破坏这些文件。

使用临时文件最好将文件屏蔽值改为 007，但是最保险的方式，是建立自己的临时文件和目录--$HOME/tmp，不要将重要的文件存放在公共的临时目录里。

5) UUCP 和其他网络

UUCP 命令用于将文件从一个 UNIX 系统传到另一个 UNIX 系统，通过 UUCP 传送的文件通常存于/usr/spool/uucppublic/login 目录，login 是用户的登录名，该目录存取许可为 777，通过网络传输并存放于此目录的文件属于 UUCP 所有，文件存取许可为 666 和 777，用户应当通过 UUCP 对传送的文件加密，并尽快移到自己的目录中去。

其他网络将文件传送到用户的 HOME 目录下的 rjc 目录中。该目录应对其他人是可写可搜索的，但是不必是可读取的，因此用户的 rjc 目录的存取许可方式为 733，允许程序在其中建立文件。同样，传送的文件也应该加密，并尽快移到自己的目录中去。

6) 特洛伊木马

在 UNIX 系统安全中，用特洛伊木马来代表某种程序，这种程序在完成某种具有明显意图的功能时，还破坏用户的安全。如果 PATH 设置为先搜索系统目录，则受特洛伊木马的攻击会大大减少，如模拟的 crypt 程序。

7) 诱骗

类似于特洛伊木马，模拟一些东西使用户泄露一些保密信息，不同的是，它由某人执行，等待无警觉的用户上当，如模拟 login。

8) 计算机病毒

计算机病毒通过把其他程序编程病毒从而传染系统，它可以迅速地扩散。特别是系统管理员由于粗心大意，作为 root 运行一些被感染的程序的时候，病毒就会大面积感染其他的程序和文件。

实验表明，一个病毒可以在一个小时内(平均少于 30 分钟)取得 root 权限。

9) 注销登录

如果用户离开自己已经登录的终端，务必要记住注销登录。

10) 智能终端

由于智能终端有 send 和 enter 换码序列，告诉终端发送当前行给系统，就像用户从键盘输入的一样，这是一种威胁的做法。非法入侵者可以用 write 命令发送信息给本用户终端，信息中包含如下的换码序列。

- 移动光标到新行(换行)。
- 在屏幕上显示“rm –r *”。
- 将该行发送给系统。

后果大家可想而知，禁止其他用户发送信息的命令是 mesg，mesgn 不允许其他用户发送信息，mesgy 允许其他用户发信息。

即使如此，仍然是有换码序列的问题存在，任何一个用户用 mail 命令发送同样一组换码序列，不同的要用! rm-r 替换 rm –r*.mal。将以!开头的行解释为一条 shell 命令，启动 shell，由 shell 解释该行的其他部分，这被称为 shell 换码。为了避免 mail 命令送换码序列到自己的终端，可以建立一个过滤程序，在读 mail 文件之前先运行过滤程序，对 mail 文件进行如下的处理：

```
myname= “$LOGNAME”;

Tr-d [\001 - \007 ][ - \013- \037]<

/usr/mail/$myname>>$HOME/mailbox;

>/usr/mail/$myname;

Mail –f $HOME/mailbox
```

其中 tr 是个字符过滤器，其输入的数据经过指定的转换后，再导向标准输出流。

11) 断开与系统的联接

用户应在看到系统确认用户登录注销后才离开计算机，以免在用户未注销时被人乘虚而入。

12) cu 命令

该命令使用户能从一个 UNIX 系统登录到另一个 UNIX 系统，此时，在远程系统中注销用户后还必须输入“~”然后回车，以断开 cu 和远程系统的联接。cu 还有两个安全的问题。

- 如本机安全性弱于远程计算机，不提倡用 cu 去登录远程机器，以免由于本机的不安全影响到较安全的远程计算机。
- 由于cu 的老版本处理“~”的方法不完善，从安全性强的系统调用安全性弱的系统时，会使弱系统的用户使用强系统的用户的 cu 传送强系统的/etc/passwd 文件，除非确信正在使用的 cu 是正确版本，否则不要调用弱系统。

10. 保护账户安全的要点

1) 保证密码的安全

- 不要将密码写下来。
- 不要选取显而易见的信息作密码。
- 不要让他人知道自己的密码。

- 不要交替使用两个不变的密码。
- 不要在不同系统上使用同样的密码。
- 不要让他人看见自己输入的密码。

2) 不让自己的文件或目录被他人写

- 如果不信任本组其他用户，umask 设置为 022。
- 确保自己的.profile 除了自己之外，其他人都不可读写。
- 暂存目录最好不存放重要文件。
- 确保 HOME 目录对任何人不可写。
- uucp 传输的文件应该加密，并尽量私人化。

3) 不让其他用户读自己的文件或目录

- umask 设置为 006 或 007。
- 如果不允许同组用户存取自己的文件和目录，umask 设置为 077。
- 暂存文件按当前的 umask 设置，存放重要数据到暂存文件的程序，就被写成能确保暂存文件对其他用户不可读。
- 确保 HOME 目录对每个用户不可读。

4) 不要设置 SUID/SGID 权限

5) 小心拷贝和移动文件

- cp 拷贝文件时，目的文件的许可方式将和文件相同，包括 SUID/SGID 许可在内，如目的文件已经存在，则目的文件的存取许可和所有者均不变。
- mv 移动文件时，目的文件的许可方式将和文件相同，包括 SUID/SGID 许可在内，如果在同一文件系统内移动文件，目的文件的所有者和小组都不变，否则，目的文件、所有者和小组将设置成本用户的有效 UID 和 GID。
- 小心使用 cpio 命令，它能覆盖不在本用户当前目录结构中的文件，可以用 t 选项首先列出要被拷贝的文件。

6) 删除 SUID/SGID 程序

删除一个 SUID/SGID 程序时，先检查程序的连接数，如果有多个链，则将该存取许可方式改为 000，然后再删除该程序；或者先写空该程序，再删除；也可将该程序的 i 结点号给系统管理员，用来查找该文件的其他链。

7) 用 crypt 加密

将一些不想让其他用户，包括超级用户看到的文件，用 crypt 命令加密。

- 不要将关键词作为命令的变量。
- 用 ed –x 或者 vi –x 编辑加密文件。

8) 除了信任的用户外，不要运行其他用户的程序，避免恶意程序被执行

9) 在自己的 PATH 系统变量中，加入系统目录，防止其他程序仿冒成系统程序

10) 不要离开自己正在登录状态的终端，以免未授权的用户对终端进行操作

11) 如果有智能终端，当心来自其他用户，包括 write、mail 命令和其他用户文件的信息中，带有换码的序列

12) 用 Ctrl+D 或者 exit 退出后，在断开与系统的连接前等待看到“login:”提示

13) 注意 cu 的版本

- 不要用 cu 调用安全性更强的系统。
- 除非确信 cu 不会被诱骗发送文件，否则不要用 cu 调用安全性较弱的系统。

4.3.2　UNIX 操作系统登录过程

当 UNIX 系统启动时，UNIX 内核将被调入计算机内存，并一直保留在内存中直到机器关闭。在引导过程中，init 程序将进入后台进行，一直到机器关闭。该程序查询文件/etc/inittab，该文件列出了连接终端的各个端口及其特征。当发现一个活动的终端时，init 程序调用 getty 程序在终端上显示 login 等待登录信息。在输入密码验证后，getty 调用 login 进程，该进程根据文件/etc/passwd 和/etc/shadow 的内容来验证用户的身份。如果用户通过身份验证，login 进程把用户的 home 目录设置成当前目录并把控制权交给一系列 setup 程序。setup 程序可以是指定的应用程序，通常作为一个 shell 程序，如：/bin/sh。得到控制后，shell 程序读取并执行文件/etc/.profile 以及.profile，这两个文件分别建立了系统范围内的和该用户自己的工作环境。最后 shell 显示命令提示符，如$。

4.4　Linux 操作系统

UNIX 系统对计算机硬件的要求比较高，对于一般的个人用户来说，想要在 PC 机上运行 UNIX 系统是比较困难的。而 Linux 就为一般用户提供了使用 UNIX 操作系统的机会。因为 Linux 是按照 UNIX 风格设计的操作系统，所以在源代码上兼容大部分的 UNIX 标准，可以说相当多的网络安全人员在自己的计算机上运行的都是 Linux。

4.4.1　Linux 操作系统简介

Linux 是在 1990 年，由芬兰赫尔辛基大学的一名学生莱纳斯 • 托瓦茨(Linus Torvalds)开发的。在 Linux 0.02 版本中已经可以运行 bash(Shell 的一种)和 gcc(GNUC 的编译器)。

最近几年 Linux 的发展和推广速度迅猛，已经有超过其他操作系统的趋势，在网络服务器领域占领了 20%的市场份额。Linux 具有与 UNIX 高度兼容、稳定性和可靠性高、源代码开放和价格低廉、安全等特点。正是由于 Linux 的源程序代码是开放式的，从而学习者可以阅读到操作系统的核心代码，有兴趣的用户甚至可以了解到整个操作系统是怎么编写的。因此在 Linux 下搞开发与在 Windows 上从事开发完全不同。因为如果在 Windows 上从事开发，可以很容易地找到 Borland 公司或者微软公司的带有友好图形界面的开发工具，但是接触不到底层的技术核心，不明白操作系统的底层连接是如何实现的。在 UNIX 上开发和 Linux 上也有所不同，在 UNIX 上开发需要一台 SUN 或者 IBM 的工作站，而 Linux 可以在个人计算机上进行。此外，Linux 有诸如 gcc 编译器等众多的免费资源可以利用，极大地降低了开发成本，也是它得以广为流传的一个主要原因。

Linux 和 Windows NT 比起来技术上存在很多优势，最主要体现在三个方面：Linux 更加

安全；Linux 更加稳定；Linux 的硬件资源占用比 Windows NT 少很多。在安全问题上，首先是针对 Linux 的病毒非常少。用户经常会碰到这样的现象，就是运行 Windows NT 的服务器时，每个星期都会由于故障而重新启动一次机器，而运行 Linux 的机器很少发生这样的故障。原因是 Linux 在稳定性上确实比 Windows 胜出一筹。在资源占用率方面，Linux 和 Windows NT 的差距超出人们的想象。一台运行 Windows NT 的服务器可以支持 50 个用户登录使用，而同一台 PC 服务器如果换成了 Linux，则可以支持 1000 名用户使用。由此算来，使用 Windows NT 和使用 Linux 的成本差异则有 20 倍之大。

Red Hat 推出的 Red Hat Linux Advanced Server 产品，是第一种企业级的 Linux 操作系统。Red Hat Linux Advanced Server 操作系统能够保证大型企业尽快从昂贵的 UNIX 操作系统中解脱出来，转移到非经济实用的 Linux 系统中。IDC 公司的一个分析数据表明，在 Internet/Intranet 环境中使用 Linux 与使用 Risc/UNIX 相比，每个使用者成本降低一半，而在合作计算任务的环境下，成本更可以节省 75%以上，这是一个相当诱人的数据。

目前国内一些小型网站很流行使用 Linux，配合 Apache 做服务器端，PHP 做开发工具，MySQL 作为数据库，这种组合对于那些以节省开支为目的，而又具有一定实用性的小型网站来说，确实有着微软的 Windows 2000+IIS+Exchange Server+SQL Server 无可比拟的优势。

4.4.2 Linux 网络安全

Linux 提供了大量的与网络安全有关的工具，但是如果运用不当，这些工具会给系统留下一些安全隐患。

近几年来 Internet 变得越来越不安全，网络的通信量日益加大，越来越多的重要交易通过网络完成，与此同时，数据被破坏、截取和修改的风险也在增加。因此，优秀的系统应当拥有完善的安全措施，应当足够抵抗来自 Internet 的侵袭。这正是 Linux 之所以流行，受到广大用户青睐的原因，并且逐渐成为 Internet 的骨干力量之一。下面我们介绍一些基本的 Linux 网络安全知识。

远程攻击者会用各种方法入侵目标的机器，他们经常寻找并利用现有程序中的漏洞，其中操作系统的漏洞更是非法入侵的必须的研究对象。相对于 Windows 操作系统，Linux 由于其开放式的源代码，可以供众多的用户和程序员进行研究和测试，总是能够快速发现这些问题并发布修补漏洞的补丁，因此 Linux 补丁的发布速度通常要比其他操作系统针对类似问题的反应要快得多。下面讲述几种入侵及反入侵，击败入侵者阴谋，构造真正安全的 Linux 系统的方法。

1. 网络服务

作为一种服务器操作系统，Linux 提供了 FTP、WWW、E-mail 等各种各样的 Internet 服务。Linux 管理大多数这类服务的方法是通过一个端口体系实现，例如 FTP 使用端口为 21。如果用户有兴趣可以尝试一下，在/etc/services 文件找到一个端口号和服务器的名字的列表清单。为了节约系统资源，简化管理操作，许多服务器都通过配置文件/etc/inetd.conf 来控制，/etc/inetd.conf 文件告诉系统怎样运行各个服务器。

2. 检查系统中运行的服务

许多开发商在 inetd.conf 的默认设置中运行了大量的服务，从尽可能安全的角度来看，它们当中的许多服务都是不必要的，应该关闭以减少被非法入侵者利用进行攻击的危险程度。

要检查 Linux 系统当前运行了哪些服务，可以输入以下命令。

```
netstat –vat
```

该命令的输出如下。

```
tcp 0 0 *:5000 *:* LISTEN

tcp 0 0 *:ww *:* LISTEN

tcp 0 0 *:auth *:* LISTEN

tcp 0 0 *:finger *:* LISTEN

tcp 0 0 *:shell *:* LISTEN

tcp 0 0 *:sunrpc *:* LISTEN
```

每一个带有“LISTEN”的行，意思为监听，代表一个正等待连接的服务，这些服务中有一部分以独立程序的形式运行，但其中大部分都由/etc/inetd.conf 控制。如果不能肯定某个服务的具体情况，请查一下/etc/inetd.conf。如：

```
grep &single;^finger&single;/etc/inetd.conf
```

上述命令从 inetd.conf 中返回如下的内容：

```
finger steam tcp nowait nobody/usr/sbin/tcpd/usr/sbin/in.fingerd
```

如果觉得并不需要这个服务，可以通过在/etc/inetd.conf 中修改相关设置关闭它：首先注释掉该行内容(在行的前面加一个“#”，即为注释标记)，然后执行命令 killall –HUP inetd，这样就关闭了一个服务，系统不需要重新启动，即时生效。

如果某个服务并没有在/etc/inetd.conf 内列出，很有可能它是一个独立的服务程序。独立服务程序提供的服务，可以通过反安装软件包删除。需要注意的是：只有用户能够肯定自己了解该程序的作用，而且确实不需要该服务的时候才可以执行删除操作，否则引发的后果有可能很严重。

3. 允许/拒绝服务器

为了进一步加强各种服务的安全性，Linux 提供了一个允许或禁止它们选择服务器的机制。/etc/hosts.allow 和/etc/hosts.deny 这两个文件中列出了服务器和服务的信任和拒绝的关系表，具体内容请参看相关的技术手册。

4. ssh(安全 Shell)

通过检查服务器名字拒绝连接是一种很好的基本攻击防范手段，但是仅仅有这一个方法是不够的，因为连接请求中的服务器名字有可能是伪造的。当数据在 Internet 上的两个程序之间传输时，它同时也处在危险当中。任何懂得这方面知识的人都可以偷看到这些数据，使用一种称为“IP 欺骗”的技术，甚至还可以将伪造的数据注入原来的数据当中。产生这些问题的原因在于 Internet 协议的作用方式。为了解决这些难题，人们设计出了 ssh。

ssh 是一种优秀的连接加密和验证系统。加密是指传输数据的时候用密钥加以保护，验证是一种检验数据包或者连接是否合法的操作。大多数操作系统都有 ssh 客户端。使用 Linux 作为服务器，可以为所有的网络应用提供 ssl 级别的安全。

5. 监视程序和运行日志

Linux 为系统管理员了解系统所发生的事情提供了一组精简的程序。下面介绍有关日志记录的工具。检查这些工具是否已经正确地安装，以及发现可入侵企图时可以查看系统日志文件。记录事件日志的主要问题在于记录的数据往往太多，因此设置好过滤条件、只记录关键信息是非常重要的。

6. jail

jail 是 Just Another IP Logger 的第一个字母缩写。它由两个后台运行的小程序组成：icmplog 和 tcplog。jail 会在/var/log/syslog 里记录用户想要了解的数据包。详情请参考相关的技术手册。

7. ftpd、rlogind 以及其他用户交互

大多数标准服务还会在/var/log/syslog 和/var/log/messages 中记录有关用户或者连接企图的信息。

利用 swatch 可以实现 syslog 文件的自动监视，swatch 不断在 syslog 中扫描系统管理员指定的事件，一旦发现需要注意的问题就发出警报。

8. 其他安全措施：防火墙

计算机中的防火墙，是一种用来保护私有网络(内部网)不受外界攻击的设备。最简单的防火墙，可以是一个带有两个网卡的 Linux 机器，其中一个网卡(以太网卡或 Modem)连接 Internet，另一个网卡连接私有网络，受保护的网络不能直接访问 Internet，Internet 也不能直接访问受保护的网络内部机器。

所有发送到或者来自 Internet(或 Intranet 网内)的数据都经过防火墙的过滤。在内部网络，像关闭某些服务之类的问题不再重要。这种方式集中了大部分力量使得某一台机器更加安全，然后用它来保护内部网络的其他机器。如何正确地配置并运行防火墙，是一个较为复杂的问题，除了要安装好机器上的两个网卡之外，还必须使用 ipchains 程序设置过滤条件。

提高系统安全性的主要缺点在于它会降低系统的可访问性(易访问性)。Linux 提供了大量的安全工具，合理地综合运用这些工具应该可以获得可访问性和安全之间的一个平衡。

9. 其他安全问题及解决方法

Linux 系统存在的一个弱点是：它使那些心怀不轨的计算机使用者可以获得防护性防火墙软件的许可，进入那些本来受到保护的网络当中。Linux 内核从 2.4.14 版本一直到 2.4.18-pre9 版本都存在这个缺陷，它存在于 netfilter 防火墙软件的一个组件当中，这个组件在两个计算机用户使用 IRS(Internet Relay System)直接进行聊天时会被用到。网上传输的信息都被分割成很多小小的“数据报”，每个数据报都带有来源地和目的地址等信息，从而指明是谁发出来的数据，以及这些数据是发送给谁的。所谓的防火墙软件就是通过发送人的地址来传输或筛选出这些数据报。Netfilter 是 Linux 内核 2.4 版本的新特点之一，是一种在内核内部运行、过滤掉不需要的数据报的软件。但是 Netfilter 的 IRC 助手组件对防火墙的设置太宽松，有可能允许来自那些本该被封掉的 IP 地址的信息。Linux 系统的龙头老大 Red Hat 公司推出的 7.1 和 7.2 版本也有这个缺陷。官方表示，存在缺陷的软件在 Red Hat 的 Linux 系统当中并不是默认安装的，但是一些用户可能会选择安装这个软件，从而带来安全隐患问题。解决的方法，最显而易见的就是，不要安装这个软件，或者去厂家网站里下载补丁。

4.5　操作系统漏洞

一般来说，黑客攻击或者入侵的行为分为两种：主动方式和被动方式。

主动方式即利用互联网可交互的特点，在网上发布一些含有恶意代码的网页、软件、电子邮件，当其他用户浏览网页、下载运行软件或者打开含有恶意代码的电子邮件时，这些代码就在目标计算机中激活，发挥作用，感染系统或者留下后门程序，以达到控制该计算机的目的。

两种入侵方式中，主动入侵的危害性更大。主动方式一般都利用了操作系统的缺陷或者漏洞，在用户不知不觉中就侵入了操作系统，获得系统的控制权。对于一般用户而言，这些攻击防不胜防。

曾经有一段时间非常猖狂的 Nimda 病毒，就是利用了 Windows 操作系统的一个漏洞，使全球许多计算机用户深受其害，造成了巨大的经济损失。操作系统的缺陷主要来源于四个方面：I/O(输入/输出)；访问策略的混乱；不完全的介入；以及通用性方面的漏洞。下面我们从操作系统的脆弱性等级划分着手，探讨一下与操作系统漏洞相关的一些问题。

4.5.1　操作系统脆弱性等级

操作系统的脆弱性可以分为 A、B、C 三个等级。

1. A 级

A 级是指允许过程用户未经授权访问的漏洞，这一类级别威胁性最大，一般来源于系统管理或者设置上的失误。

2. B 级

B 级是指允许本地用户非法访问的漏洞，允许本地用户获得或增加未经授权的访问。这类级别威胁性处于中等，主要来源于应用程序，例如缓冲区的溢出。缓冲区是内存中存放临时数据的地方。当程序试图将数据放到计算机内存中的某个位置，如果计算机没有足够的内存空间，将发生缓冲区溢出。

目前，防止缓冲区溢出的方法通常有以下几种。

1) 编写正确的代码

编写正确的代码是一件重要而耗时的工作，特别是编写汇编等语言的程序，一行代码的错误也许就导致整个程序的致命错误。

2) 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。事实上，很多老的 UNIX 系统都是这样设计的，但是近来的 UNIX 和 Windows 系统为了实现更好的性能和功能，往往在数据段中动态放入可以执行的代码，例如调用 DLL(动态链接库)的函数等。

3) 数组边界检查

植入代码引起缓冲区溢出是一个问题，扰乱程序的正常执行流程是另一个问题。不像非执行缓冲区保护，数组边界检查完全避免了数据缓冲区的溢出以及因此而产生的攻击。这样，只要数组不溢出，溢出攻击就无从谈起了。为了实现数组边界检查，所有对数组的读写操作都应当被检查，以确保对数组的操作控制在准确的范围之内。

4) 程序指针完整性检查

程序指针完整性检查和边界检查略有不同，与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即使一个攻击者成功地改变程序的指针，由于系统事先检测到了指针的改变，这个指针也不会被使用。与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题。采用其他的缓冲区溢出方法可以避免这种检测，并且这种方法在性能上有很大的优势，兼容性也很好。

3. C 级

C 级是指允许拒绝服务(DoS)的漏洞。这类级别威胁性最小，一般来源于操作系统本身。

拒绝服务的英文全称是 Denial of Services。从网络攻击的各种方法和它们产生的破坏情况来看，DoS 算是一种很简单而有效的进攻方式。它的目的就是拒绝用户的服务请求，破坏组织的正常运作，最终它会使得部分 Internet 连接和网络系统失效。最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，致使服务超载，无法响应其他请求。

这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者内部连接。这些攻击会导致资源的匮乏，无论计算机的处理速度有多快，内存容量有多大，互联网的速度有多快，都无法避免这些攻击带来的严重后果。

4.5.2　操作系统漏洞

操作系统的漏洞是指非法用户未经授权获得访问或者提高访问权限的硬件或者软件特征，漏洞是一种形式的脆弱性。下面通过几种具有代表性的攻击来探讨与系统漏洞相关的问题。

1. 口令的攻击术

黑客攻击目标时常把破译普通用户的口令作为攻击的开始。先用“finger 远端主机名”找出主机上的用户账户，然后采用字典穷举法进行攻击。它的原理是：网络上的用户常采用英语单词或自己的姓氏作为口令。通过一些程序，自动从电脑字典中取出一个单词，作为用户的口令输入给远端的主机，申请进入系统。若口令错误，就按顺序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令，或者把字典的单词试完为止。由于这个破译过程由计算机程序自动完成，几个小时就可以把字典的所有单词试完，这一类程序的典型代表是 Let Me Inversion。

如果这种方法不能奏效，黑客就会仔细寻找目标的薄弱环节和漏洞，伺机夺取目标中存放口令的文件 shadow 或 passwd。因为在现代的 UNIX 操作系统中，用户的基本信息存放在 passwd 中，而所有的口令都经过 DES 加密算法加密后专门存放在一个叫 shadow(影子)的文件中，并处于严密的保护之中。老版本的 UNIX 没有 shadow 文件，它所有的口令都放在 passwd 文件中，一旦窃取了口令文件，黑客就会用专门破解 DES 算法的程序来破译用户密码。

系统管理员也应该定期运行一些破译口令的工具，来尝试破译 shadow 文件，如果有用户的口令密码被破译出，说明这些用户的密码设置过于简单，或者长期没有更改，或者是有一定的规律和个人特征相联系，容易被黑客利用作为突破口，管理员应该及时通知这些用户，及时修改密码，以防止被不法入侵者利用。

2. IIS Unicode 漏洞攻击

1) IIS Unicode 漏洞描述

微软 IIS 4.0 和 IIS 5.0 在 Unicode 字符编码的实现中存在一个安全漏洞，导致用户可以远程通过 IIS 执行任意命令。当 IIS 打开文件时，如果该文件包含 Unicode 字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致 IIS 错误的打开或者执行某些 Web 根目录以外的文件。

对于 IIS 5.0/4.0 中文版，当 IIS 收到的 URL 请求的文件名里包含有一个特殊的编码，例如：“%c1%hh”或者“%c0%hh”，它会首先将其编码变成：0xc10xhh，然后尝试打开这个文件。Windows 系统认为 0xc10xhh 可能是 Unicode 编码，因此它会首先对其解码，如果 0x00<=%hh<0x40 的话，采用的解码格式与下面的类似：

%c1%hh → (0xc1-0xc0) * 0x40 + 0xhh

%c0%hh → (0xc0-0xc0) * 0x40 + 0xhh

IIS 其他版本也受影响，但是 unicode 编码相应的有所不同。Windows NT 4.0 编码为：%c1%9c，Windows 2000 英文版编码为：%c0%af。

2) 攻击程序

攻击程序相对简单，通过 TCP Socket 建立 HTTP 连接，从命令行界面搜集命令，并根据

目标服务器的 IIS 版本不同，构造和发送 GET 命令，然后获取 IIS 的反馈信息，利用这些信息进行下一步入侵的操作。

下面举例来说明一个攻击的实例。

(1) 测试环境

- 攻击平台：Windows 2000 Server。
- 目标机器：Windows 2000 Server 简体中文版(包含 IIS 5.0)。

(2) 攻击方法

- 运行 iisunicode.exe <目标机 IP/域名>。
- 选择目标机 IIS 版本。
- 在 cmd>提示符下输入在目标机上运行的命令，回车结束。
- 程序打印目标机的返回结果，回到 cmd>提示符下接收下一条命令。
- 在 cmd>下输入 quit 退出程序。

本 章 小 结

本章主要介绍了各种操作系统的安全问题，包括以下主要内容。

4.1、4.2 节着重说明了 Windows 系统的安全基础，并以 Windows 98/ME、Windows 2000/NT/XP 为例子，列举了一些系统的安全漏洞，探讨了相关的解决方法，以及 Windows 系统的安全管理问题。

4.3 节介绍 UNIX 系统的基本知识、文件系统和用户管理等，讨论了一些系统的网络安全问题及解决方法，以及系统的安全管理问题。

4.4 节主要介绍了 Linux 系统的网络安全基础、安全漏洞及解决方法等。

4.5 节介绍了操作系统常见的漏洞，以及可能被攻击的情形。

课 后 练 习

一、 填空题

1. Windows 98 系统有三种登录方式，分别是(　　　　　)、(　　　　　)、(　　　　　)。

2. NTFS 可以使用大于(　　　　　)B 的卷，FAT 文件容量最大为(　　　　　)B，FAT32 在 Windows XP 中，只能格式化最多(　　　　　)B 的卷。

3. Windows NT 4.0 中主要的分布式安全协议是(　　　　　)；而在 Windows 2000 中，(　　　　　)是缺省的分布式安全协议。

4. 在 UNIX 操作系统登录过程中，login 进程根据文件(　　　　　)和(　　　　　)的内容来验证用户的身份。

5. 操作系统的脆弱性可以分为(　　　　　)、(　　　　　)、(　　　　　)三个等级，其中(　　　　　)类级别的威胁性最大。

二、 选择题

1. Windows 98 系统的登录方式中，最不安全的方式是(　　)。
   A. Windows 登录　B. 网络用户登录　C. 友好用户登录　D. 远程登录
2. 以下几种文件格式中，最大文件长度不能超过 2GB 的是(　　)，最大文件长度不能超过 4GB 的是(　　)。
   A. NTFS　B. FAT　C. FAT 32　D. HFS
3. 以下几种措施中，不属于修改注册表信息来提高 Windows 98 安全性的是(　　)。
   A. 禁止非法用户登录　B. 隐藏或禁止访问控制面板
   C. 禁止访问注册表编辑器　D. 禁止网络用户登录方式
4. Windows NT 系统上的重大安全漏洞主要体现在(　　)方面。
   A. 浏览器的安全漏洞　B. NT 服务器的漏洞
   C. NT 工作站的漏洞　D. NT 系统的漏洞
5. UNIX 操作系统的安全焦点是(　　)，其中包括(　　)。
   A. 文件许可权　B. 读许可权　C. 写许可权　D. 执行许可权

三、 简答题

1. 为什么说 Windows 98 的注册表很重要？如何提高 Windows 98 的安全性？
2. 为了加强 Windows 2000 账户的登录安全性，应做哪些方面的工作(即账户的登录策略)。
3. Windows NT/2000/XP 系统的缺陷漏洞有哪些？
4. UNIX 系统有哪些安全漏洞？可用什么方法来防范？
5. Linux 系统为何会成为当前主流的网络操作系统？

第5章　密码学基础

随着计算机犯罪和网络犯罪案例的不断增加，计算机和网络安全逐渐成为一个重大的社会问题。在这样的大环境下，作为最早的安全防范研究课题的计算机密码学，走出了军方的专用领域，逐步转向教育、科研和民用领域，成为保证计算机安全的一项重要技术措施，这使得信息加密解密技术的研究成为计算机科学工作者所关注的重要研究领域。

密码学分为密码编译和密码分析两个分支，密码编码学是对信息进行编码以实现隐蔽信息的一门学科，而密码分析学则是研究分析破译密码的学科，两者相互对立而又相互促进。本章以密码学的基础为重点，介绍相关的概念、算法以及密码学的发展史。

本章重点

- 古典密码学
- 对称密码算法
- 非对称密码算法
- 数字签名
- PGP 原理与应用

5.1　概　　述

密码学是一门深奥的数学学科，密码学协议为安全通信提供了坚定的基石。密码技术是研究数据加密、解密及变换的科学，涉及数学、计算机科学、电子与通讯等诸多学科。虽然其理论相当高深，但其概念却十分简单。密码技术包含两方面密切相关的内容，即加密和解密。加密就是研究、编写密码系统，把数据和信息转换成不可识别的密文的过程；而解密就是研究密码系统的加密途径，恢复数据和信息本来面目的过程。加密和解密过程共同组成了加密系统。

在加密系统中，要加密的信息称为明文(Plan Text)，明文经过变换加密后，成为密文(Cipher Text)。由明文变成密文的过程就称为加密(Enciphering)，通常由加密算法来实现。由密文还原成明文的过程称为解密(Deciphering)，通常由解密算法来实现。为了有效控制加密和解密算法的实现，在其处理过程中，必须有通信双方共同掌握的专门信息参与其中，这种信息就被称为密钥(Key)。由此可见，对数据进行加密，是需要通过算法和密钥来实现的。

对于较为成熟的密码体系，其算法是公开的，密钥是保密的。这样使用者简单地修改密

钥，就可以达到改变加密过程和加密结果的目的。通常密钥由一个小字符串组成，它可以选择多种功能的加密方法中的一种，并且可以按照需要频繁更换。

5.1.1　密码学的历史

密码是一门古老的技术，它已经有几千年的历史，自从人类社会有了战争就出现了密码。最先有意识地使用一些技术来进行加密信息的，应该是公元前的古希腊人。他们使用一种双方都知道长度和宽度的棍子，把信息纵向写在棍子上，用纸把棍子裹起来，信息就可以印在了纸上。如果不知道棍子的长度和宽度的人，获取了这个信息，是不能正确翻译出信息的准确内容的。古代最著名的加密方法应该是凯撒大帝的 3 个字母轮换表的加密方法。

中国古代秘密通信的手段，就已经有一些近似于密码的雏形。《孙子兵法》里写道：“兵者，诡道也”。要想“诡道”成功，就必须注意信息保密。宋代的曾公亮、丁度等编撰的《武经总要》里记载，北宋时期，在作战中曾用一首五言律诗的 40 个汉字分别代表 40 种情况或者要求，这种加密方式已经具有了密码机制的特点。

在欧洲，公元前 405 年，斯巴达的将领们便使用了原始的密码；公元前一世纪古罗马皇帝凯撒曾使用有序的单字表代替密码；之后逐步发展为密本、多表代替以及加乱等各种加密体制。

1871 年，由上海大北水线电报公司选用 6899 个汉字，代替四码数字，成为中国最初的商业明码本，同时也涉及了由明码本改编为密本及进行加乱的方法。

20 世纪初，产生了最初的可以使用的机械式和电机式密码机，同时出现了商业密码机公司和市场。20 世纪 60 年代后，电子密码机得到了较快的发展和广泛的应用。

20 世纪 70 年代以来，一些学者提出了公开密钥体制，即运用单向函数的数学原理，以实现加、脱密密钥的分离。加密密钥是公开的，脱密密钥是保密的。这种新的密码体制，引起了密码学界的广泛关注和讨论。

密码破译是随着密码的广泛使用而逐步产生和发展的。1412 年，波斯人卡勒卡尚迪所编的百科全书中，记载有破译简单的代替密码的方法。到 16 世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信，破译密码技术有了相当的发展。1863 年普鲁士人卡西斯基所著的《密码和破译技术》，以及 1883 年法国人克尔克霍夫所写的《军事密码学》等书籍文献，都对密码学的理论和方法做过一些论述和讨论。1949 年美国人 Shannon 发表了《秘密体制的通信理论》一文，应用信息论的原理分析了密码学中的一些基本问题。

自 19 世纪以来，由于电报特别是无线电报的广泛使用，为密码通信和第三者的截获，提供了极为有利的条件。通信保密和破译展开了一场持久的、激烈的信息隐蔽战争。1917 年，英国破译了德国外长齐默尔曼的电报，导致了美国对德宣战。1942 年，美国从破译的日本海军电报中，获悉日军对中途岛地区的作战计划和兵力部署，扭转了太平洋地区的战局。在保卫英伦三岛和其他许多的著名历史战役中，密码破译的成功显示了极其重要的战略意义，这些事例也从侧面说明了密码破译的重要军事地位和意义。

20 世纪五六十年代，电脑开始发展，在计算机的计算中有一种“模 2 加”运算，程序成为“异或”计算，如果配合二进制换位运算，就可以很容易实现信息加密和解密的功能。

进入20世纪70年代之后，密码学迎来了新纪元，开创了现代密码学。具有代表意义的是：1975年3月，IBM公司公开发表了DES数据加密标准；1977年，美国国家标准局(ANSI)宣布DES作为国家标准用于非国家保密机关，开创了公开全部密码算法的先例；1976年，Diffie和Hellam提出不仅密码本身可以公开，而且加密密钥也是可以公开的，只要解密密钥保持其隐秘性就可以确保信息传输的安全和可靠，这就是加密密钥和解密密钥不同的非对称密码体系，又称为公钥密码体系；1978年，Rivest、Shamir和Adleman三人合作，提出了第一个适用的公钥密码算法，即著名的RSA密码算法。一直到现在，DES和RSA两个密码算法都是现代密码学的经典范例。

当今世界，主要国家的政府和军队都十分重视密码工作，有的设立庞大机构，从财政预算里拨出巨额的经费，集中数以万计的专家和科技人员，投入大量的昂贵的计算机和其他电子设备进行研究工作。

5.1.2　密码学的定义

密码学这个词是从两个意思为“密码书写”的希腊字演变而来的，它是一门隐匿消息的艺术和科学。密码分析，就是破解密码，密码学的基础部件是密码系统。

密码学的目标是保持加密信息的机密性。假设一个攻击者希望破解一段密文，标准的密码学方法假设他知道加密明文的算法，而不知道具体的密钥，那么他可能通过以下三种方式进行攻击。

1. 惟密文攻击

攻击者只拥有信息的密文，他的目的是找到相应的明文。

2. 已知明文攻击

攻击者拥有密文和这些密文对应的明文，目的是找到以上明文密文所用过的密钥。

3. 选择明文攻击

攻击者可以对一些特定的明文进行加密，可以得到明文所对应的密文，目的也是找到以上明文密文所用过的密钥。

一套好的密码系统应该能够抵抗以上三种类型的攻击。

5.2　密码学的基本概念

5.2.1　基本概念

密码学是研究加密和解密变换的一门科学。通常情况下，人们将可以看懂的文本称为明文，用“M”表示。需要注意的是，M可以不是ASCII码文本，它可以是任何类型的未加密数据。将明文变换成的不易看懂的文本就是密文，这个过程就叫做加密；加密的逆过程，即把密文翻译成为明文的过程，就是解密。遵循ISO 7498—2标准的定义，加密的术语称为“密

码(Encipher)”和“解译密码(Decipher)”。明文与密文的相互变换，是一个可逆的过程，并且只存在唯一的、不存在误差的可逆变换。完成加密和解密的算法称为密码体制。

加密和解密的过程可以用图 5-1 来表示。

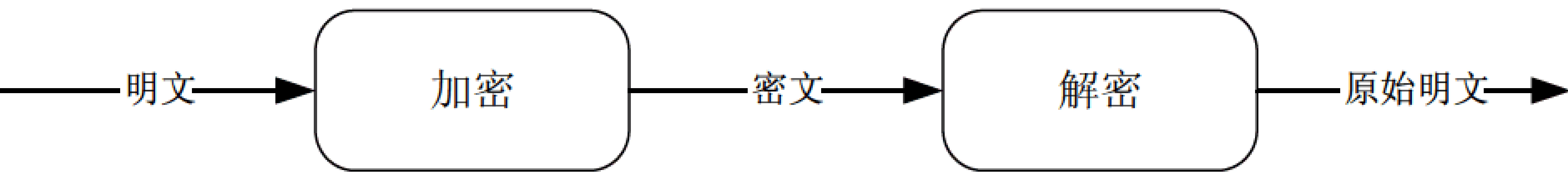


图 5-1　加密和解密

使消息保密的科学和技术叫做密码编码学，从事此行业的专业人员叫密码编码者或者密码程序员。密码分析者是从事密码分析的专业人员，密码分析学就是破译密文的科学和技术。作为数学的一个分支的密码学，包括密码编码学和密码分析学两个方面，精于此道的人称为密码学家，现代的密码学家通常也是理论数学家。

明文用 M(消息)或者 P(明文)表示。对于计算机专业的理解，P 是简单的二进制数据，明文可以被传送或者存储，无论在哪种情况，M 指待加密的消息。

密文用 C 来表示，它也是二进制数据，有时候和 M 一样大，有时候稍微大一些，具体情况视加密的算法而定，有时候通过一定的算法压缩后，C 也可能比 P 要小一些。加密函数 E 作用于 M 得到密文 C，用数学公式表示为：

$$E(M) = C$$

相反的，解密函数 D 作用于 C 产生 M：

$$D(C) = M$$

先加密后解密消息，原始的明文就会被回复，下面的等式必须成立：

$$D(E(M)) = M$$

意思即为：加密算法和解密算法是一个可逆的过程。

5.2.2　密码系统的安全性

密码算法是用于加密和解密的数学函数，通常情况下，有两个相关的函数：一个用于加密，一个用于解密。

如果算法的保密性是基于保持算法的秘密和安全，这种算法称为受限制的算法。如果有人无意中暴露了这个算法的秘密，所有人都必须改变之前的算法。更加糟糕的是，受限制的密码算法不可能进行质量控制或标准化。因为每个组织和用户必须有他们各自的特有算法，而尽可能地避免与别人的相同。

尽管有一些或多或少的缺陷，受限制的算法对于低安全级别的应用来说还是足以应付的，用户也许并没有意识到，或者压根不在乎他们系统中存在的那些问题。

现代密码学，用密钥来解决了这个问题，密钥用 K(Key)来表示。K 可以是很多数值里的任意值。密钥 K 的可能值的范围叫做密钥空间。加密和解密算法都使用这个密钥(即运算都依赖于密钥，并用 K 表示)，这样，加密和解密的过程则变成如图 5-2 所示。

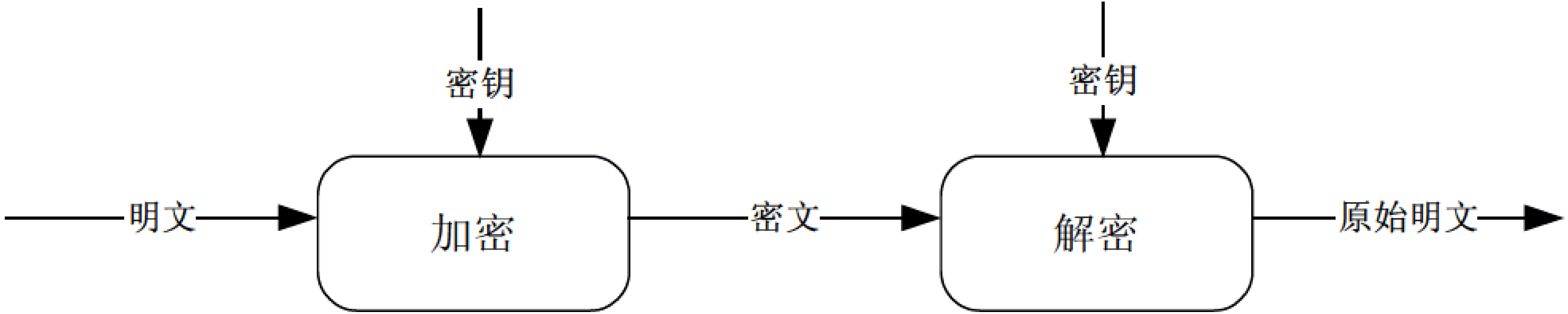


图 5-2　使用同一个密钥的加密解密

有些算法里，加密和解密的程序使用不同的密钥进行相关的计算，也就是说加密密钥(我们称为 K1)和解密密钥(我们这里姑且称为 K2)可以不同，情况如图 5-3 所示。

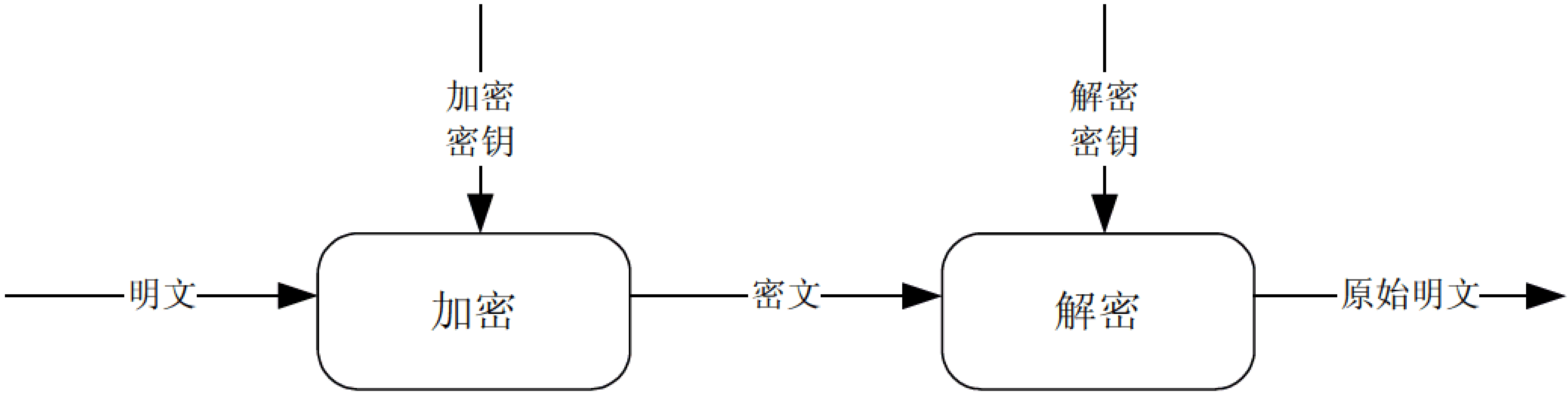


图 5-3　使用两个不同密钥的加密解密

所有这些算法的安全性都基于密钥的安全性，而不是基于算法的细节的安全性。这就意味着算法可以公开，也可以被分析，可以大量生产使用算法的产品，即便窃听者知道了算法也没有关系只要不知道具体的密钥，就无法得知信息的真实内容。

5.2.3　密码体制分类

密码系统由算法以及所有可能的明文、密文、密钥组成。基于密钥的算法通常有两类：对称算法和公开密钥算法。对称算法有时又叫传统密码算法，就是加密密钥能够从解密密钥中推算出来，反之亦然。在大多数对称算法中，加密、解密密钥是相同的。这些算法也叫秘密密钥算法或者单密密钥算法，它要求发送者和接收者在安全通信之前，协商确定一个密钥。对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都能对信息进行加密和解密，只要通信需要保密，密钥就必须保密。

对称算法可以分为两类：一类只对明文的单个比特，有时候也针对字节，运算的算法称为序列算法或者序列密码。另一类算法是对明文的一组比特进行运算，这些比特组称为分组，相应的算法称为分组算法或者分组密码。

公开密钥算法，也叫非对称算法。它的设计思路是：用于加密的密钥不同于用于解密的密钥，而且解密密钥不能根据加密密钥计算出来(至少在合理假定的长时间内)。之所以叫做公开密钥算法，是因为加密密钥能够公开，即陌生人能够用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在这些系统中，加密密钥叫做公开密钥(简称公钥)，解密密钥叫做私人密钥(简称私钥)，私钥有时候也叫做秘密密钥。

5.2.4　对密码系统的攻击

对密码进行分析的尝试称为攻击。荷兰人 A.Kerckhoffs 最早在 19 世纪阐明了密码分析的一个基本假设，这个假设就是秘密必须全部包含在密钥中。Kerckhoffs 假设密码分析者已经有了密码的算法和全部实现的详细技术资料。

一般来说，常用的密码攻击有 7 类，如上所述，我们都假设密码分析者已经知道了每一类加密算法的全部技术内容。

1. 惟密文攻击

密码分析者有一些消息的密文，这些消息都是用同一个加密算法加密。

2. 已知明文攻击

密码分析者不仅可以得到一些消息的密文，而且也知道这些消息的明文。

3. 选择明文攻击

分析者不仅可以得到一些消息的密文和相应的明文，而且也可选择被加密的明文。

4. 自适应明文攻击

这是选择明文攻击的特殊情况。密码分析者不仅能够选择被加密的明文，也能基于以前加密的结果修正这个选择。

5. 选择密文攻击

密码分析者能够选择不同的被加密的密文，并可以得到对应的解密的明文。

6. 选择密钥攻击

这种攻击并不表示密码分析者能够选择密钥，它只表示密码分析者具备不同密钥之间的关系的相关知识。这种方法有些奇特，不是非常切合实际。

7. 软磨硬泡(Rubber-hose)攻击

密码分析者威胁、勒索或折磨某人，直到获取破解密码系统的密钥为止。

已知明文攻击和选择性明文攻击，比人们想象中的还要常见。已知明文攻击在二战中已经被成功地用来破译敌国的密码，例如德国和日本的密码系统。

需要着重指出的是，切记 Kerckhoffs 的假设：如果在设计密码系统的时候，将新的密码系统设计成为高度依赖于攻击者不知道算法的机制，这样的系统注定会失败。历史上这样的教训已经不少，1994 年 RC4 算法就被人破译了。最好的算法是那些已经被相关机构公开，并经过世界上最好的密码分析家们多年的攻击，仍然不能破译的算法。

5.3　古典密码学

5.3.1　凯撒密码

凯撒密码是最古老的替换密码，据说是 Julius Casesar 发明的，因此而得名。替换密码是用一组密文字母来代替一组明文字母的隐藏明文的方法，这种加密方法保持明文字母的排列位置不变。以英文字母为例，它把 D 换成 a，E 换成了 b，F 换成了 c，以此类推……也就是

说密文的字母相对于明文字母循环移动 3 个位置，因此，凯撒密码又被称为循环移位密码。如果将凯撒加密法通用化，即允许加密字母不仅移动 3 个位置，而是可以移动用户自定义的 N 个位置，在这样的情况下，N 就是通常加密算法里的密钥，也就是这个循环移位密码中的密钥 K。这种密码的优点是，密钥简单，易于记忆，但是由于明文和密文的对应关系过于简单，所以安全性也较差。

5.3.2　仿射密码

对于凯撒密码的一种改进方法是：使明文字母和密文字母之间的映射关系没有一定的规律可循。例如，将 26 个字母，都映射成另外的字母，如表 5-1 所示。

表 5-1　单字母映射表

明文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密文	W	Q	R	E	Y	T	O	I	A	P	S	D	F	G	H	J	K	X	Z	V	C	B	N	M	U	L

另一种更加复杂的映射方式，是由一个不同字母组成的单词或者少于 26 个字母的字符串，例如，密钥为 JUSTIN，那么就会得到表 5-2 所示的映射关系。

表 5-2　某个单词或字母串为密钥的映射表

明文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密文	J	U	S	T	I	N	A	B	C	D	E	F	G	H	K	L	M	O	P	Q	R	V	W	X	Y	Z

不过，如果给出一段密文，还是可以找到一些破解的突破口。一种最显而易见的方法是猜测明文中可能出现的单词或者短语。有重复模式的单词以及使用频率很高的单词，以及常用作起始和结束的字母都可以给破译者猜测字母排序的一些线索。另一种方法是利用自然语言的统计数据，根据使用和组合的概率的高低进行筛选。由于替换密码是明文字母与密文字母之间的一一映射，所以在密文中仍然保存了明文中字母的分布和出现概率，这就使得这种加密方法的安全性大大降低。

5.3.3　维吉尼亚密码

针对上述密码算法的不足，一种改进的算法应运而生，它就是 Vigenere 密码(维吉尼亚密码)。Vigenere 密码利用长密钥可以隐匿消息的统计特性，选择一个密钥序列，该密钥序列用一个字符串表示。密钥的字母作用于对应的明文字母，当到达密钥的最后一个字母时，密钥又重新对应后面的明文。密钥的长度成为密文的周期。表 5-3 给出一个表格结构，用于快速有效的加密。因为 Vigenere 密码需要几个不同的字母作为密钥，所以这种形式的密码称为

多字母替换密码。

表 5-3　Vigenere 密码表格

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

我们举一个实例来说明这个密码表的用法：选择如下一行句子，并且用密钥“WORLD”作为加密密钥，那么获得的密文如下所示。

密钥：WORL DW ORLD W ORL DW ORLDWORLD

明文：L I FE　I S LIKE　A BOX OF CHOCOLATE

密文：HWWP LO ZZVH W PFI RB QYZGKZREH

重合指数用于测量密文中的字母频率的差异，它被定义为从密文中随机选择的两个字母可能相同的概率。重合指数越低，则表明密文字母变化越少，密文的周期也越长，这里探讨的是英文的语言模式。

多年以来，Vigenere 密码曾经一度被认为是不可被破解的。后来一名普鲁士骑兵军官 Kasiski 发现，当密钥的字母重复出现在相同的字符上时，密文字母会发生重复，重复字母之间的字母数是密文周期的倍数，因而 Vigenere 密码的破解也是有迹可循的。

实验证明，简单的 Vigenere 密码是可以通过手算破解的；但是对于复杂的密码，攻击方法就只能通过计算机计算来实现。

5.3.4　Playfair 密码

与上述的 Vigenere 密码一样，Playfair 密码也是一种多字母代替密码，区别是 Playfair 密码用的是二字母代替密码。

Playfair 密码是英国曾在第一次世界大战期间使用过的一种二字母代替密码。Playfair 密码密钥由 25 个英文字母(J 与 I 相同)组成的五阶方阵如表 5-4 所示。

表 5-4　Playfair 密码的密钥方阵

H	A	R	P	S
I	C	O	D	B
E	F	G	K	L
M	N	Q	T	U
V	W	X	Y	Z

每一对明文字母 M_1 和 M_2 都根据下面 6 条规则进行加密。

1. 规则一

若 M_1 和 M_2 在密钥方阵中的同一行，则密文字母 C_1 和 C_2 分别是 M_1 和 M_2 右边的字母(第一列视为在第五列的右边)。

2. 规则二

如果 M_1 和 M_2 在同一列，则 C_1 和 C_2 分别是 M_1 和 M_2 下面的字母。

3. 规则三

如果 M_1 和 M_2 位于不同的行和列，则 C_1 和 C_2 是以 M_1 和 M_2 为顶点组成的长方形中的另外两个顶点。其中 C_1 和 M_2、C_1 和 M_2 分别在同一行。

4. 规则四

如果 M_1=M_2，那么 M_1 和 M_2 之间插进一个无效字母，例如可以为 X。

5. 规则五

如果明文信息一共有奇数个字母，那么在明文的末尾加上一个无效字母。

6. 规则六

字母 I 和 J 可看成是同一个字母。

举一个例子，假设明文为 Computer，用 Playfair 法加密的结果则如下。

明文：CO MP UT ER

密文：OD TH MU GH

5.3.5　Hill 密码

Hill 密码也叫方程加密法，是 Hill 发明的以联立方程为基础的加密法，因此而得名。用 X 表示明文，Y 表示密文字母。其数字可以根据表 5-5 中的任意建立的字母来定义。

表 5-5　Hill 密码字母表

字母	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
数字	4	8	25	2	9	20	16	5	17	3	0	22	13	24	6	21	15	23	19	12	7	11	18	1	14	10

算法规定，加密序列以四个明文字母为一组，所以加密算法可以用四元方程组来表示，因此此算法又称为四元代替法，加密时用下列的加密方程。

$Y_1=8X_1+6X_2+9X_3 5X_4 \quad MOD\ 26$

$Y_2=6X_1+9X_2+5X_3+10X_4 \quad MOD\ 26$

$Y_3=5X_1+8X_2+4X_3+9X_4 \quad MOD\ 26$

$Y_4=10X_1+6X_2+11X_3+4X_4 \quad MOD\ 26$

根据加密方程，可以得到解密方程的公式如下。

$X_1=23Y_1+20Y_2+5Y_3+1Y_4 \quad MOD\ 26$

$X_2=2Y_1+11Y_2+18Y_3+1Y_4 \quad MOD\ 26$

$X_3=2Y_1+20Y_2+6Y_3+25Y_4 \quad MOD\ 26$

$X_4=25Y_1+2Y_2+22Y_3+25Y_4 \quad MOD\ 26$

举一个实例，假设给明文 HELP 加密。

首先，根据解密公式可以将明文变换成一组数字。

H　$X_1=5$

E　$X_2=9$

L　$X_3=22$

P　$X_4=21$

用加密算法方程组加密。

$Y_1=7$

$Y_2=15$

$Y_3=10$

$Y_4=14$

再译成字母，密文就是 UQZY，解密时用解密方程组进行计算就可以得到原明文。

5.4　对称密码算法

5.4.1　对称密码算法概述

如前文所述：对称算法有时又叫传统密码算法，就是加密密钥能够从解密密钥中推算出来，反之亦然。在大多数对称算法中，加密、解密密钥是相同的。这些算法也叫秘密密钥算法或者单密密钥算法，它要求发送者和接收者在安全通信之前，协商确定一个密钥。对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都能对信息进行加密和解密，只要通信需要保密，密钥就必须保密。下面介绍几种常见的对称密码算法。

5.4.2　DES 算法

数据加密标准(Data Encryption Standard，DES)是美国国家标准局于 1977 年公布的由 IBM 公司研制的加密算法。DES 算法被授权用于所有非保密的通信场合，后来还曾被国际标准组织采纳为国际标准。DES 算法是一种典型的按分组方式工作的单密钥密码算法，它的基本思想是将一个二进制序列的明文分组，然后用密钥对该明文进行替代和置换，最后得到密文。DES 算法是对称的，既可以用于加密也可以用于解密。它的巧妙之处在于，除了密钥输入顺序之外，加密和解密的步骤几乎完全相同，从而在制作 DES 硬件芯片时很容易实现标准化和通用化，很符合现代通信和批量生产的需要。

DES 算法将输入的明文分为 64 位的数据分组，使用 64 位的密钥进行变换，每个 64 位的明文分组数据经过初始置换、16 次迭代和逆置换这三个主要的步骤，最后输出得到 64 位的密文。在迭代之前，首先要对 64 位的密钥进行变换，密钥去掉第 8、第 16、第 24 到第 64 位减少至 56 位，去掉的那 8 位视为奇偶校验位，不包含有密钥信息，所以实际的密钥长度只有 56 位。DES 算法的加密流程如图 5-4 所示。

DES 算法的初始置换过程为：输入 64 位明文，按初始置换规则把输入的 64 位数据按位重新组合，并把输出分为左右两部分，每部分长度为 32 位。在这里用到的初始置换规则如表 5-6 所示。

这个置换表的含义是：将输入的第 58 位换到第 1 位，第 50 位换到第 2 位，第 42 位换到第 3 位，以此类推……最后一位是原来的第 7 位。也就是说，置换前的位置分别是 $D_1D_2D_3 \cdots\cdots D_{64}$，那么经过初始置换之后，左边部分为 $D_{58}D_{50}D_{42} \cdots\cdots D_8$，就是表 5-6 的上半部分数据；右边部分为 $D_{57}D_{49}D_{41} \cdots\cdots D_7$，也就是表 5-6 的下半部分数据。具体位置请参看表 5-6 的相应位置的数值。

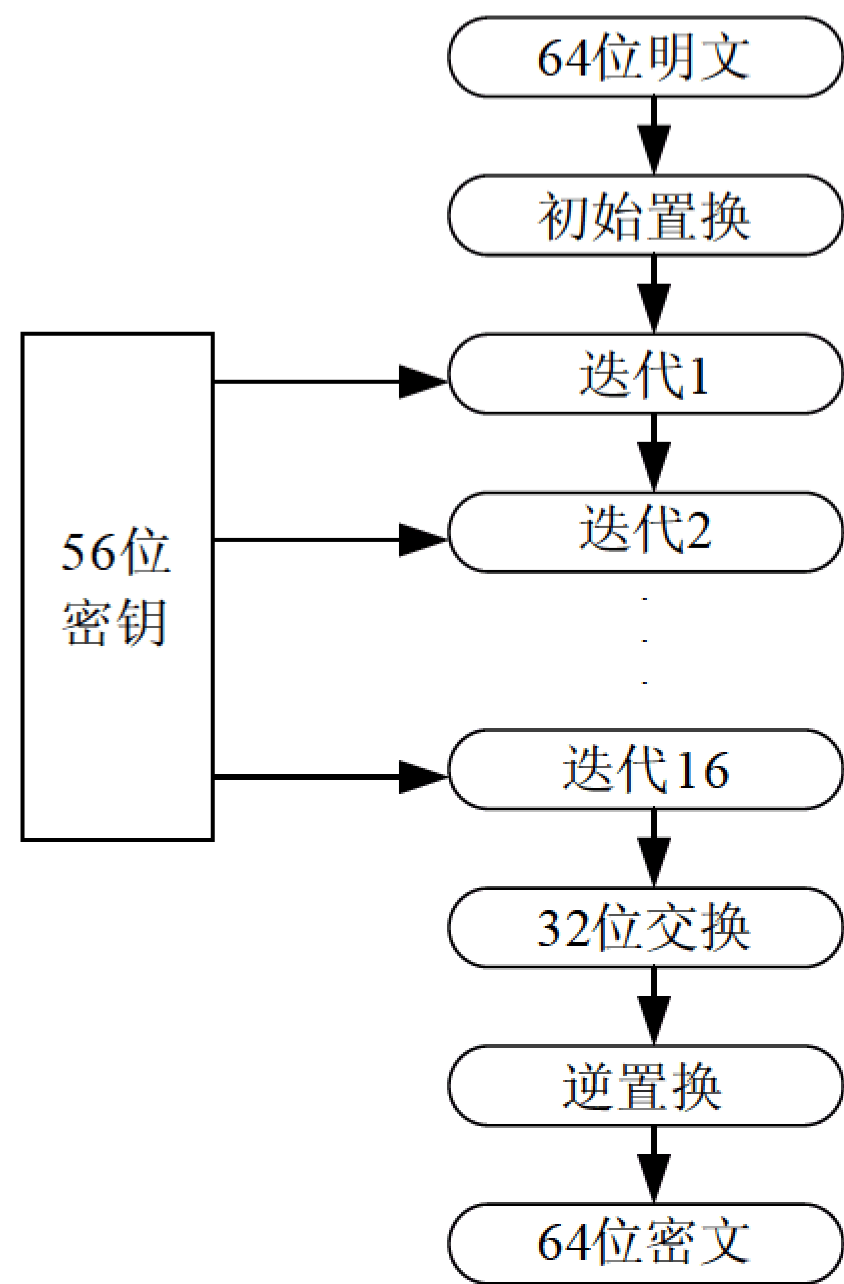


图 5-4　DES 加密过程

表 5-6　初始置换规则表

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

这个置换表的含义是：将输入的第 58 位换到第 1 位，第 50 位换到第 2 位，第 42 位换到第 3 位，以此类推……最后一位是原来的第 7 位。也就是说，置换前的位置分别是 $D_1D_2D_3$……D_{64}，经过初始置换之后，左边部分为 $D_{58}D_{50}D_{42}$……D_8，就是表 5-6 的上半部分数据；右边部分为 $D_{57}D_{49}D_{41}$……D_7，也就是表 5-6 的下半部分数据。具体位置请参看表 5-6 的相应位置的数值。

每个迭代过程实际上包括四个独立的操作。首先是右半部分由 32 位扩展为 48 位，然后与密钥的某一个形式组合，其结果被替换成另一个结果，同时其位数又压缩到了 32 位。这 32 位数据经过置换再与其左半部分相加，结果产生新的右半部分。

每一个右半部分都经过扩展排列，由 32 位扩展为 48 位。扩展过程置换位的顺序的同时，也重复了某些位。扩展的目的有两个：使得密文中间结果的一半与密钥相匹配；产生一个较长的结果后又将其压缩。扩展排列由表 5-7 定义，由于是扩展排列，所以有些位将不止移至一个输出位上。

表 5-7　扩展排列表

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

由于每隔 8 位删除一位，64 位的密钥变成 56 位，56 位的密钥经过 PC-1 置换，输出顺序如表 5-8 所示。

表 5-8　PC-1 置换表

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

在一轮的每一步，密钥被分成包含各 28 位的两个部分，每个部分都左移由一个十进制数指明的若干位，然后将两部分评介起来。随后对 56 位进行置换，作为该轮的密钥。每轮的密钥与经过扩展来自上面的右半部分进行异或相加。

在每一轮中，密钥的两个半部分独立地循环左移，移动次数由一个指定的数字来决定。表 5-9 为各轮需要移动的位数。

表 5-9　各轮移动的位数表

轮次	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

移位之后，从 56 位中抽取 48 位用作与已扩展的右半部分相异或，表 5-10 给出了选择 48 位的排列。

表 5-10　选择排列表

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

至此，得到 48 位的数据，再将这 48 位按顺序分成 8 组，每组 6 位，这 8 组分别通过变换，由每组输入 6 位变成每组输出 4 位，从而得到 32 位的数据。这个 32 位的数据再经过 P 置换，P 置换的置换表如表 5-11 所示。

表 5-11　P 置换表

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

至此，整个加密过程完成。DES 的解密过程和 DES 加密类似，只是将 16 轮的子密钥序列 $K_1,K_2,\ldots,K_{16}$ 的顺序颠倒过来使用，即第一轮使用 K_{16}，第二轮使用 K_{15}，第 16 轮使用 K_1，证明的过程在此不再赘述，有兴趣的读者可以查阅相关技术文献。

5.4.3　AES 算法

传统的 DES 由于只有 56 位的密钥，因此已经不适应当今分布式开放网络对数据加密安全性的要求。1997 年 RSA 数据安全公司发起了一项“DES 挑战赛”的活动，志愿者四次分别用四个月、41 天、56 个小时和 22 个小时破解了其用 56 位密钥 DES 算法加密的密文。即 DES 加密算法在计算机速度提升后的今天被认为是不安全的。因此，寻找一种可以替代 DES 的新加密算法已经势在必行。

密码学中的高级加密标准(Advanced Encryption Standard，AES)，又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。AES 是美国国家标准技术研究所(NIST)旨在取代 DES 的 21 世纪的加密标准。

AES 是美国联邦政府采用的商业及政府数据加密标准，预计将在未来几十年里代替 DES 在各个领域中得到广泛应用。AES 提供 128 位密钥，因此，128 位 AES 的加密强度是 56 位 DES 加密强度的 1021 倍还多。假设可以制造一部可以在 1 秒内破解 DES 密码的机器，那么使用这台机器破解一个 128 位 AES 密码需要大约 149 亿万年的时间。更深一步比较而言，宇宙一般被认为存在了还不到 200 亿年。因此可以预计，美国国家标准局倡导的 AES 即将作为新标准取代 DES。

经过 5 年的甄选流程，高级加密标准由美国国家标准与技术研究院 (NIST)于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

AES 的基本要求是，采用对称分组密码体制，密钥长度的最少支持为 128、192、256，分组长度 128 位，算法应易于各种硬件和软件实现。1998 年 NIST 开始 AES 第一轮分析、测试和征集，共产生了 15 个候选算法。1999 年 3 月完成了第二轮 AES2 的分析、测试。2000 年 10 月 2 日美国政府正式宣布选中比利时密码学家 Joan Daemen 和 Vincent Rijmen 提出的一种密码算法 Rijndael 作为 AES。

AES 加密数据块大小最大是 256 位，但是密钥大小在理论上没有上限。AES 加密有很多轮的重复和变换。大致步骤为：密钥扩展(Key Expansion)；初始轮(Initial Round)；重复轮(Rounds)，每一轮又包括 SubBytes、ShiftRows、MixColumns、AddRoundKey；最终轮(Final Round)，最终轮没有 MixColumns。

尽管人们对 AES 还有不同的看法，但总体来说，AES 作为新一代的数据加密标准，汇聚了强安全性、高性能、高效率、易用和灵活等优点。AES 设计有三个密钥长度：128、192、256 位。相对而言，AES 的 128 密钥比 DES 的 56 密钥强 1021 倍。AES 算法主要包括三个方面：轮变化、圈数和密钥扩展。本文以 128 为例，介绍算法的基本原理，并结合 AVR 汇编语言，实现高级数据加密算法 AES。

AES 是分组密钥，算法输入 128 位数据，密钥长度也是 128 位。用 N_r 表示对一个数据分组加密的轮数。每一轮都需要一个与输入分组具有相同长度的扩展密钥 Expandedkey(i)的参予。由于外部输入的加密密钥 K 长度有限，所以在算法中要用一个密钥扩展程序(Key Expansion)把外部密钥 K 扩展成更长的比特串，以生成各轮的加密和解密密钥。

1. 圈变换

AES 每一个圈变换由以下三个层组成。

非线性层：进行 Subbyte 变换。

线行混合层：进行 ShiftRow 和 MixColumn 运算。

密钥加层：进行 AddRoundKey 运算。

2. 轮变化

对不同的分组长度，其对应的轮变化次数是不同的。

3. 密钥扩展

AES 算法利用外部输入密钥K(密钥串的字数为N_k)，通过密钥的扩展程序得到共计$4(N_{r+1})$字的扩展密钥。它涉及如下三个模块。

- 位置变换(Rotword)——把一个 4 字节的序列[A，B，C，D]变化成[B，C，D，A]。
- S 盒变换(Subword)——对一个 4 字节进行 S 盒代替。
- 变换 Rcon——Rcon 表示 32 位比特字[x_{i-1}，00，00，00]。这里的 x 是(02)，如 Rcon[1]=[01000000]；Rcon[2]=[02000000]；Rcon[3]=[04000000]……扩展密钥的生成：扩展密钥的前 N_k 个字就是外部密钥 K；以后的字 W[]等于它前一个字 W[[I－1]]与前第 N_k 个字 W[[I－N_k]]的“异或”，即 W[]=W[[I－1]]W[[I－N_k]]。但是若 i 为 N_k 的倍数，则 W=W[I－N_k]Subword(Rotword(W[[I－1]]))Rcon[i/N_k]。

5.4.4　分组密码工作模式

传统密码学一般包括序列加密、分组加密。序列密码一直是军事和外交场合使用的主要密码技术之一。它的主要原理是：通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流，得到密文序列。所以，序列密码算法的安全强度完全取决于它所产生的伪随机序列的好坏。

分组密码的工作方式是将明文分成固定长度的组，如 64 或者 32、48 比特一组，用同一个密钥和算法对每一块进行加密和解密，输出也是固定长度的密文，上面介绍的 DES 密码算法就是这种类型。

对称密码体制的发展趋势将以分组密码为重点。分组密码算法通常由密钥扩展算法和加密(解密)算法两部分组成。密钥扩展算法将 b 字节用户主密钥扩展成 r 个子密钥。加密算法由一个密码学上的弱函数 f 与 r 个子密钥迭代 r 次组成。混乱和密钥扩散是分组密码算法设计的基本原则。抵御已知明文的差分和线性攻击，可变长密钥和分组是该体制的设计要点。

这种工作模式存在的主要问题是：由于加密、解密双方都要使用相同的密钥，因此在发送、接收数据之前，必须完成密钥的分发。所以，密钥的分发便成了该加密体系中的最薄弱环节，也是风险最大的环节，所使用的手段都很难保障安全地完成整个工作。这样，密钥的更新周期加长，给非法破译密钥提供的机会也越大。

5.4.5　Java 中的对称密码算法编程实例

下面我们以 IDEA 算法为例，介绍用 Java 实现该算法的编程实例。

先简单介绍一下 IDEA 加密算法的原理：IDEA 数据加密算法是由中国著名学者来学嘉博士和著名的密码学专家 James L. Massey 于 1990 年联合提出的。它的明文和密文都是 64 比特，但是密钥长 128 比特。IDEA 是作为迭代的分组密码实现的，它使用 128 位的密钥和 8 个循环。这比 DES 提供了更多的安全性，但是在选择用于 IDEA 的密钥时，应该排除那些称为“弱密钥”的密钥。DES 只有 4 个弱密钥和 12 个次弱密钥，而 IDEA 中的弱密钥数相当可观，有 2 的 51 次方个。但是如果密钥的总数非常大，达到 2 的 128 次方个时，仍有 2 的 77 次方个密钥可供选择。IDEA 被认为是极为安全的。使用 128 位密钥，蛮力攻击中需要进

行的测试次数和 DES 相比会明显增大，甚至允许对弱密钥进行测试，而且它本身也显示了抵抗专业形式的分析攻击的能力。

Java 密码体系(JCA)和 Java 扩展密码(JCE)的设计目的是为 Java 提供与实现无关的加密函数 API。它们都用 Factory 方法来创建类的例程，然后把实际的加密函数委托给提供者提供指定的底层引擎，引擎中为类提供了接口在 Java 中实现数据的加密和解密，是使用其内置的 JCE 来实现的。Java 开发工具集 1.1 为实现包括数字签名和信息摘要在内的加密功能，推出了一套基于供应商的新型灵活应用编程接口。Java 密码体系结构支持供应商的互操作，同时支持硬件和软件实现。Java 密码学结构设计遵循两个原则。

- 算法的独立性和可靠性。
- 实现的独立性和相互作用性。

算法的独立性是通过定义密码服务类来获得。用户只需了解密码算法的概念，而不用去关心如何实现这些代码。密码服务提供器是实现一个或者多个密码服务的一个或多个程序包。软件开发商根据一定接口，将各种算法实现后，打包成一个文件，用户可以安装和配置这些文件，可以将这些.ZIP 或者.JAR 文件放在 CLASSPATH 目录下，再编辑 JAVA 安全属性文件来设置定义。

下面是一个实例演示。

```
//加密过程的实现
void idea_enc(int data11[], int key1[])   //待加密的 64 位数据首地址
{
    int i;
    int tmp,x;
    int zz[]= new int[6];
    for(i=0; i<48; i+=6) //循环 8 轮
    {
        for( int j=0, box=I; j<6; j++,box++)
        {
            zz[j]= keyl[box];
        }
        x=handle_data(data11,zz);
        tmp=data11[1]; //交换中间两数值
        data11[1]=data11[2];
        data11[2]=tmp;
    }
    tmp=data11[1[;//最后一轮不交换
    data11[1]=data11[2];
    data11[2]=tmp;
    data11[0]=MUL(data11[0],key1[48]);
    data11[1]=(char)((data11[1]+key1[49])% 0X10000);
    data11[2]=(char)((data11[2]+key1[50])% 0X10000);
    data11[3]=MUL(data11[3],key1[51]);
}
```

5.5　非对称密码算法

5.5.1　非对称密码算法概述

上面介绍的几种算法，构成了“传统密码体制”，又称“对称密钥密码体制”。其中用于加密的密钥和解密的密钥完全一样，在对称密钥密码体制中，加密运算与解密运算使用同样的密钥。通常，使用的加密算法比较简便高效，密钥简短，破译极其困难。但是在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。1976 年，Diffie 和 Hellman 为了解决密钥管理问题，在他们具有奠基性意义的著作“密码学的新方向”一文中，提出了一种密钥交换协议，允许在不安全的媒体上通信双方交换信息，安全地达成一致的密钥。在此新思想的基础上，很快出现了与“传统密码体制”相对应的“非对称密钥密码体制”，即“公开密钥密码体制”。其中加密密钥不同于解密密钥，加密密钥公之于众，谁都可以用；而解密密钥只有解密人自己知道。这两个密钥分别称为“公开密钥”(Public Key)和“秘密密钥”(Private Key)。

非对称密钥密码体制是现代密码学的最重要发明和进步。在一贯的印象当中，密码学(Cryptography)或称密码术主题应该是保护信息传递的机密性。的确，保护敏感的通讯，一直是密码学多年来的重点。但是，这仅仅是当今密码学主题的一个方面。随着网络应用的普及和迅速发展，对信息发送人的身份验证，成为密码学主题的另一个方面。公开密钥密码体制为这两方面的问题都给出了出色的答案，并在继续产生新的思想和方案。

下面以 RSA 算法为例，介绍一下这种机制的工作原理。

5.5.2　RSA 算法

RSA 公开密钥算法是由麻省理工学院(MIT)R.Rivest、A.Shamir 和 L.Adleman 三名数学家于 1977 年提出的。RSA 的取名就来自于这三个发明者的姓的第一个字母。后来，他们在 1982 年创办了以 RSA 命名的公司 RSA Data Security Inc.和 RSA 实验室，该公司和实验室在公开密钥密码系统的研究和商业推广方面具有举足轻重的地位，是迄今为止最为成功的公开密钥密码体制。

现在用一个简单的例子来说明 RSA 公开密钥算法的工作原理。取两个质数 p=11，q=13，p 和 q 的乘积为 p×q=143，算出另一个数 z=(p-1)×(q-1)=120；再选取一个与 z 互质的数字，例如：e=7(称为“公开指数”)，对于这个 e 值，可以算出另一个值 d=103(称为“秘密指数”)满足 e×d=1 mod z；其实 7×103=721 除以 120 的余数的确是 1。(n，e)和(n，d)这两组数分别为“公开密钥”和“秘密密钥”。

设想 S 需要向 Y 发送机密信息 s(明文，即未加密的报文)，S 已经从公开媒体中得到了 Y 的公开密钥(n，e)=(143，7)，于是可以算出加密值为：

c = s[RUe] mod n = 85[RU7] mod 143 = 123

将 c 发送给 Y，Y 在收到“密文”(即加密过的报文)c=123 之后，利用只有 Y 自己知道的秘密密钥(n，d)= (143，123)计算出来 123 mod 143，得到的值就是明文 85，这一个过程就是解密过程。其中的计算用一般公式来表示就是：

C[RUd] mod n = (s[RUe])[RUd] mod n = s[RUed] mod n

根据初等数论中的欧拉定理(Euler)，应用 s[RUz] = 1 mod n，得到：

S[RUed] = s mod n

所以，Y 可以得到 S 发给他的真正信息 s=85。

也许有一些人会产生疑问：在 Y 向公众提供了公开密钥，密文 c 又是通过公开的途径传送的，那么其安全性何在？回答是：只要 n 足够大，例如 512 比特，或者 1024 比特甚至 2048 比特，n = p×q 中的 p 和 q 相差位数不大，任何人只知道公开密钥(n，e)，目前是无法算出秘密密钥(n，d)的。其困难在于从乘积 n 难以找到它的两个巨大的质数因子。

公开密钥加密系统的一个优点是不仅可以用于信息的保密通讯，而且可以用来验证信息发送者的身份(Authentication)或者数字签名(Digital Signature)。我们用一个身份验证的例子来进行说明。

Y 要向 S 发送信息 m(表示他身份的，可以是身份证号码，或者名字的汉字的某种编码值)，必须让 S 确信该信息是真实的，是由 Y 本人所发的。为此，Y 使用自己的秘密密钥(n，d)计算。

S= md mod n 建立了一个“数字签名”，通过公开的通讯途径发送给 S，S 则使用 Y 的公开密钥(n，e)对收到的 s 值进行计算。

S[RUe] mod n = (md)e mod n=m

这样，S 经过验证，知道信息 S 确实代表了 Y 的身份，只有他本人才能发出这一信息，因为只有他自己知道秘密密钥(n，d)。其他任何人即使知道 Y 的公开密钥(n，e)，也无法猜出或算出他的秘密密钥来冒充他的“签名”。

RSA 公开密码算法的安全性取决于从公开密钥(n，e)计算出秘密密钥(n，d)的困难程度，而后者则等同于从 n 找出它的两个质因数 p 和 q。因此，寻求有效的因数分解的算法就是寻求一把锐利的“矛”，来击穿 RSA 公开密钥密码系统这个“盾”。数学家和密码学家一直在努力寻求更锐利的“矛”和更坚固的“盾”，这不仅仅局限于 RSA 一种算法，对于其他算法也是如此。

最简单的考虑就是加厚“盾”的厚度，即取更大的 n 值。RSA 实验室认为，512 比特的 n 已经不够安全，他们建议个人应用需要 768 比特的 n，公司和企业应用需要 1024 比特的 n，其他极其重要的场合应该用到 2048 比特或者更大的 n。

总之，随着硬件资源的迅速发展和因数分解算法的不断改进，为了保证 RSA 密钥算法密码系统的安全性，最简明有效的做法就是不断增加模 n 的位数。

5.5.3　Java 中的非对称密码算法编程实例

下面以 RSA 算法为例子，介绍用 Java 实现该算法的编程实例。

```
//为了方便观察学习，在此程序内，我们使用相对小的大整数
import java.io.*;
import java.math.BigInteger;
import java.security.SecureRandom;
public class RSA{
```

```
private final static SecureRandom random = new SecureRandom();
private BigInteger e; //e:公钥
private BigInteger d; //d:私钥
private BigInteger n; //n:模数

RSA()
{
    SecureRandom rnd= new SecureRandom();
    BigInteger p= new BigInteger(512,10,rnd);
    BigInteger q= new BigInteger(512,10,rnd);
    while(p.equals(q))
    {
        Q=new BigInteger(512,10,rnd);
        //fin=(p-1)(q-1)
        BigInteger fin= (p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE)));
        n=p.multiply(q); //n= qp
        e= new BigInteger(20，10，rnd)；//随机选取整数 e
        //保证 e 满足 gcd(fin(n),e) = 1，即 e 与 fin(n)互素
        while((e.gcd(fin).intValue())!=1)
        {
            e =   new BigInteger(20,10,rnd);
        }
        d = e.modInverse(fin);
        System.out.println(“公钥 =”+e+“\n”);
        System.out.println(“私钥 =”+d+“\n”);
      System.out.println(“模数 n 的值= ”+n+“\n”);
    }


    BigInteger encrypt(BigInteger msg) //加密函数
    {
       reuturn msg.modPow(e,n);
    }

    BigInterger decrypt(BigInteger encrypted) //解密函数
    {
          reuturn msg.modPow(d,n);
    }

    publie static void main(String[] args)
    {
        RSA obj= new RSA();
        BigInteger msg = new BigInteger(512,random);
        BigInteger encrypt=obj.encrypt(msg); //加密
```

```
                BigInteger decrypt=obj.decrypt(encrypt); //解密
                System.out.println("原始明文="+msg+"\n");
                System.out.println("加密密文 ="+encrypt+"\n");
                System.out.println("解密明文 ="+decrypt+"\n");
            }
        }
    }
```

5.6　数 字 签 名

5.6.1　数字签名概述

签名是大家都熟悉的一种身份确认方法。计算机发展至今，由于技术上的问题，手工签名还不能在它上面很快普及，而签名被复制和伪造的可能性又大大增加，所以在计算机中处理个人确认问题一直是人们所关注的事情。

最开始普遍采用的方式是口令，用字符数字串作为个人的代号，由个人私自保管使用；同时又在计算机内以隐蔽文件的方式存储，使用时用户输入自己的口令与计算机内存放的口令直接进行比较，以确认用户的身份合法性。但是人们发现这种确认方式的安全性不高，只要稍有计算机应用知识的人，就可以比较容易弄到他人的口令。

后来又采用指定认证字的方法(相当于经过处理的口令)，问题还不能得到圆满解决。而且，即使防止了外部普通用户的假冒犯罪行为，也难以防止系统内部的管理人员(通常称为超级用户)的计算机犯罪行为，因为计算机超级用户有很高的计算机操作权限，他可以打开计算机内的任何文件，包括口令、认证字的隐蔽文件。在大量计算机犯罪案例中很多是在系统内部发生的。以上所介绍的各种认证方法，用户只有被系统检查的义务，而没有足够的自我保护的能力和权限，这是一种消极、被动的方法。

一种数字签名(又称公钥数字签名、电子签章)应运而生。数字签名是一种以电子形式存在于数据信息之中的，或者作为其附件的或逻辑上与之有联系的数据，可以用于辨别数据签署人的身份，并表明签署人对数据信息中包含的信息的认可。

数字签名不是将用户的签名扫描成数字图像，或者用触摸板获取签名的方式，更不是通常人们所说的落款签名。数字签名的文件的完整性是很容易验证的，不需要骑缝章、骑缝签名，也不需要笔迹专家鉴定，具有不可抵赖性。

简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、Des/DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可

否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。

数字签名(Digital Signature)技术是不对称加密算法的典型应用。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。数字签名必须能够保证信息传输的完整性、发送者的身份认证，防止交易中的抵赖发生。

数字签名是个加密的过程，数字签名验证是个解密的过程。

5.6.2　基于 RSA 算法的数字签名

如上一节 RSA 算法的描述，该算法的一个优点是不仅可以用于信息的保密通讯，而且可以用来验证信息发送者的身份(Authentication)或者数字签名(Digital Signature)。我们仍然可以用一个例子来进行说明。

Y 要向 S 发送信息 m(表示他身份的，可以是身份证号码或者名字的汉字的某种编码值)，必须让 S 确信该信息是真实的，是由 Y 本人所发的。为此，Y 使用自己的秘密密钥(n，d)计算。

S= md mod n 建立了一个“数字签名”，通过公开的通讯途径发送给 S，S 则使用 Y 的公开密钥(n，e)对收到的 S 值进行计算：

S[RUe] mod n = (md)e mod n=m

这样，S 经过验证，知道信息 S 确实代表了 Y 的身份，只有他本人才能发出这一信息，因为只有他自己知道秘密密钥(n，d)。其他任何人即使知道 Y 的公开密钥(n，e)，也无法猜出或算出他的秘密密钥来冒充他的“签名”。

5.6.3　Java 中的数字签名算法编程实例

JDK 1.5 提供了对 RSA 的算法支持，同时，为数字签名提供了很好的接口，java.security.Signature 类提供了消息签名。

在加密和数字签名的程序开头加入以下代码。

```
import java.security.Signature;
import java.security.KeyPairGenerator;
import java.security.KeyPair;
import java.security.SignatureException;
```

下面介绍用 Java 实现该数字签名的编程实例。

```
//数字签名，使用 RSA 私钥对消息摘要签名，然后使用公钥进行验证
public class DigitalSignature2Example
{
    public static void main(Sting[] args) throws Exception
    {
        System.err.println(“Usage: java DigitalSignature2Example”);
        System.exit(1);
        byte[] plainText=args[0].getBytes(“UTF8”);
```

```
        System.out.println("Start generating RSA key"); //生成 RSA 公钥
        KeyPairGenerator keyGen= KeyPairGenerator.getInstance("RSA");\
        keyGen.initialize(1024);
        KeyPair key=keyGen.generateKeyPair();
        System.out.println("Finish generating RSA key");
        Signature sig=Signature.getInstance("SHA1WithRSA"); //使用私钥签名
        sig.initSign(key.getPrivate());
        sig.update(plainText);
        byte[] signature=sig.sign();
        System.out.println(sg.getProvider().getInfo());
        System.out.println("Signature:");
        System.out.println(new String(signature, "UTF8"));
        System.out.println("Start signature verification"); //使用公钥验证
        sig.initVerify(key.getPublic());
        sig.update(plainText);
        try
        {
            if(sig.verify(signature))
            {
                System.out.println("Signature verified");
            }
            else System.out.println("Signature failed");
        }
        cach(SignatureException e)
        {
            System.out.println("Signature failed");
        }
    }
}
```

5.7　PGP 原理与应用

现代信息社会里，在电子邮件广受欢迎的同时，其安全性问题也很突出。实际上，电子邮件的传递过程是邮件在网络上反复复制的过程，其网络传输路径不确定，很容易遭到不明身份者的窃取、篡改、冒用甚至恶意破坏，给收发双方带来麻烦。进行信息加密，保障电子邮件的传输安全已经成为广大 E-mail 用户的迫切要求。PGP 的出现与应用很好地解决了电子邮件的安全传输问题。将传统的对称性加密与公开密钥方法结合起来，兼备了两者的优点。PGP 提供了一种机密性和鉴别的服务，支持 1024 位的公开密钥与 128 位的传统加密算法，可以用于军事目的，完全能够满足电子邮件对于安全性能的要求。

5.7.1　操作描述

PGP 的实际操作由五种服务组成：鉴别、机密性、电子邮件的兼容性、压缩、分段和重装。

1. 鉴别

如图 5-5 所示，鉴别的步骤如下。

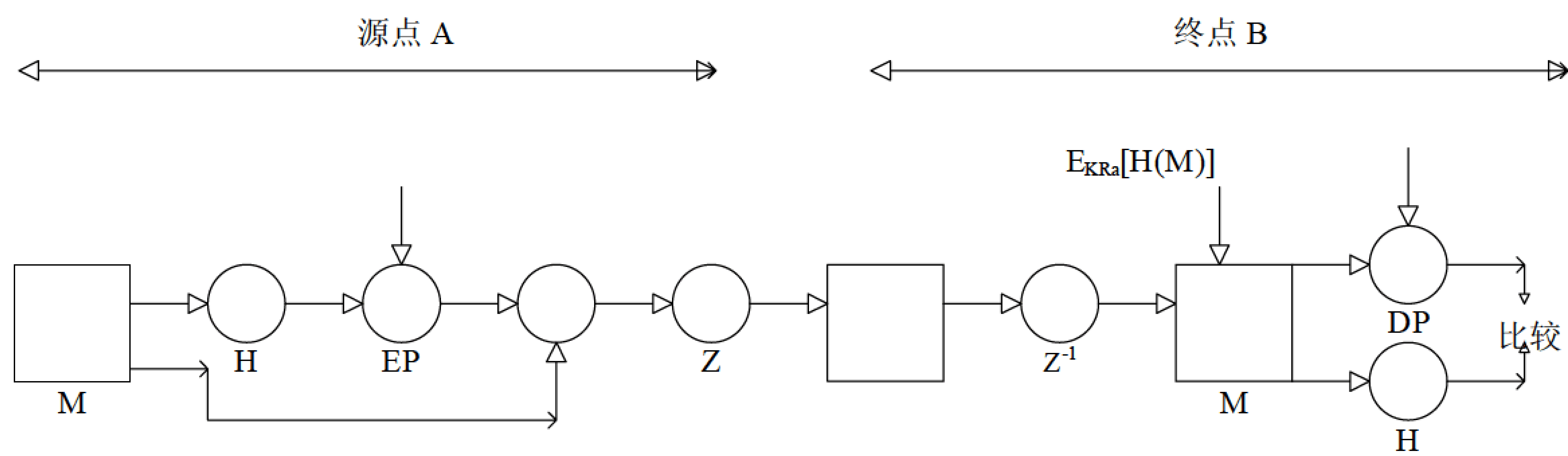


图 5-5　只进行鉴别

(1) 发送者创建报文。

(2) 发送者使用 SHA-1 生成报文的 160 位散列代码(邮件文摘)。

(3) 发送者使用自己的私有密钥，采用 RSA 算法对散列代码进行加密，串接在报文的前面。

(4) 接收者使用发送者的公开密钥，采用 RSA 解密和恢复散列代码。

(5) 接收者为报文生成新的散列代码，并与被解密的散列代码相比较。如果两者匹配，则报文作为已鉴别的报文而接收。

另外，签名是可以分离的。例如法律合同需要多方签名，每个人的签名是独立的，因而可以仅应用到文档上。

2. 机密性

在 PGP 中，每个常规密钥只使用一次，即对每个报文生成新的 128 位的随机数。为了保护密钥，使用接收者的公开密钥对它进行加密。图 5-6 显示了这一步骤，具体步骤如下。

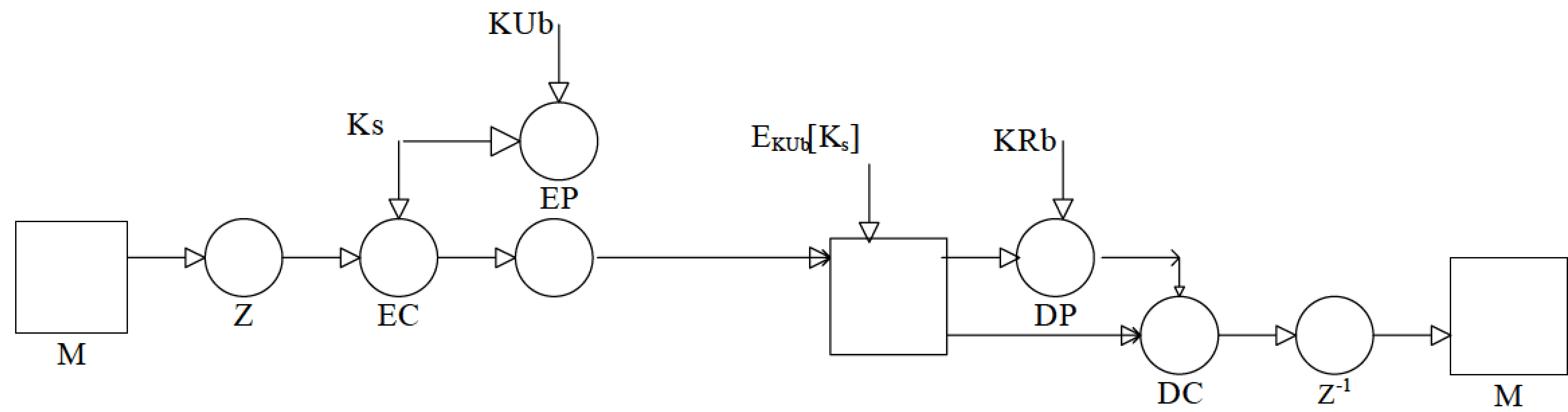


图 5-6　只保证机密性

(1) 发送者生成报文和用作该报文会话密钥的 128 位随机数。

(2) 发送者采用 CAST-128 加密算法，使用会话密钥对报文进行加密，也可使用 IDEA 或 3DES。

(3) 发送者采用 RSA 算法，使用接收者的公开密钥对会话密钥进行加密，并附加到报文前面。

(4) 接收者采用 RSA 算法，使用自己的私有密钥解密和恢复会话密钥。

(5) 接收者使用会话密钥解密报文。

除了使用 RSA 算法加密外，PGP 还提供了 Diffie Hellman 的变体 EIGamal 算法。

3. 常规加密和公开密钥加密结合的好处

(1) 常规加密和公开密钥加密结合使用比直接使用 RSA 或 EIGamal 要快得多。

(2) 使用公开密钥算法解决了会话密钥分配问题。

(3) 由于电子邮件的存储转发特性，使用握手协议来保证双方具有相同会话密钥的方法是不现实的，而使用一次性的常规密钥加强了已经很强的常规加密方法。

4. 机密性与鉴别

对报文可以同时使用两个服务。首先为明文生成签名并附加到报文首部；然后使用 CAST-128(或 IDEA、3DES)对明文报文和签名进行加密，再使用 RSA(或 EIGamal)对会话密钥进行加密。在这里要注意次序，如果先加密再签名的话，别人可以将签名去掉后签上自己的签名，从而篡改签名。

5. 电子邮件的兼容性

当使用 PGP 时，至少传输报文的一部分需要加密，因此部分或全部的结果报文由任意 8 位字节流组成。但由于很多电子邮件系统只允许使用由 ASCII 正文组成的块，所以 PGP 提供了 radix-64(就是 MIME 的 BASE 64 格式)转换方案，将原始二进制流转化为可打印的 ASCII 字符。

6. 压缩

PGP 在加密前进行预压缩处理，PGP 内核使用 PKZIP 算法压缩加密前的明文。一方面对电子邮件而言，压缩后再经过 radix-64 编码有可能比明文更短，这就节省了网络传输的时间和存储空间；另一方面，明文经过压缩，实际上相当于经过一次变换，对明文攻击的抵御能力更强。

7. 分段和重装

电子邮件设施经常受限于最大报文长度(50 000 个)八位组的限制。分段是在所有其他的处理(包括 radix-64 转换)完成后才进行的，因此，会话密钥部分和签名部分只在第一个报文段的开始位置出现一次。在接收端，PGP 必须剥掉所在的电子邮件首部，并且重新装配成原来的完整的分组。

5.7.2　加密密钥和密钥环

1. 会话密钥的生成

PGP 的会话密钥是个随机数，它是基于 ANSI X.917 的算法由随机数生成器产生的。随机数生成器从用户敲键盘的时间间隔上取得随机数种子。对于磁盘上的 randseed.bin 文件则采用和邮件同样强度的加密。这有效防止了他人从 randseed.bin 文件中分析出实际加密密钥的规律。

2. 密钥标志符

允许用户拥有多个公开/私有密钥对。

- 不时改变密钥对。
- 同一时刻，多个密钥对在不同的通信组交互，所以用户和他们的密钥对之间不存在一一对应关系。

3. 密钥环

密钥需要以一种系统化的方法来存储和组织，以便有效和高效地使用。PGP 在每个结点提供一对数据结构，一个是存储该结点年月的公开/私有密钥对(私有密钥环)；另一个是存储该结点知道的其他所有用户的公开密钥。相应地，这些数据结构被称为私有密钥环和公开密钥环。

5.7.3　公开密钥管理

1. 公开密钥管理机制

一个成熟的加密体系必然要有一个成熟的密钥管理机制配套。公钥体制的提出就是为了解决传统加密体系的密钥分配过程不安全、不方便的缺点。例如网络黑客们常用的手段之一就是“监听”，通过网络传送的密钥很容易被截获。对 PGP 来说，公钥本来就是要公开，就没有防监听的问题。但公钥的发布仍然可能存在安全性问题，例如公钥被篡改(Public Key Tampering)，使得使用公钥与公钥持有人的公钥不一致。这在公钥密码体系中是很严重的安全问题，因此必须帮助用户确信使用的公钥是与他通信的对方的公钥。

以用户 A 和用户 B 通信为例，现假设用户 A 想给用户 B 发信。首先用户 A 就必须获取用户 B 的公钥，用户 A 从 BBS 上下载或通过其他途径得到 B 的公钥，并用它加密信件发给 B。不幸的是，用户 A 和 B 都不知道，攻击者 C 潜入 BBS 或网络中，侦听或截取到用户 B 的公钥，然后在自己的 PGP 系统中以用户 B 的名字生成密钥对中的公钥，替换了用户 B 的公钥，并放在 BBS 上或直接以用户 B 的身份把更换后的用户 B 的“公钥”发给用户 A。A 用来发信的公钥是已经更改过的，实际上是 C 伪装 B 生成的另一个公钥(A 得到的 B 的公钥实际上是 C 的公钥/密钥对，用户名为 B)。这样一来，B 收到 A 的来信后就不能用自己的私钥解密了。

2. 防止篡改公钥的方法

(1) 直接从 B 手中得到其公钥，这种方法有局限性。

(2) 通过电话认证密钥：在电话上以 radix-64 的形式口述密钥或密钥指纹。密钥指纹(Keys Fingerprint)就是 PGP 生成密钥的 160 位的 SHA-1 摘要(16 个 8 位十六进制)。

(3) 从双方信任的 D 那里获得 B 的公钥。如果 A 和 B 有一个共同的朋友 D，而 D 知道他手中的 B 的公钥是正确的。D 签名的 B 的公钥上载到 BBS 上让用户去拿，A 想要获得 B 的公钥就必须先获取 D 的公钥来解密 BBS 或网上经过 D 签名的 B 的公钥，这样就等于加了双重保险，一般没有可能去篡改而不被用户发现。这就是从公共渠道传递公钥的安全手段。

(4) 由一个普通信任的机构担当第三方，即“认证机构”。这样的“认证机构”适合由非个人控制的组织或政府机构充当，来注册和管理用户的密钥对。现在已经有等级认证制定的机构存在，如广东省电子商务电子认证中心(www.cnca.net)就是一个这样的认证机构。对于那些非常分散的用户，PGP 更赞成使用私人方式的密钥转介。

3. 信任的使用

PGP 确实为公开密钥附加信任和开发信任信息提供了一种方便的方法使用信任。

公开密钥环的每个实体都是一个公开的密钥证书。与每个信任的实体相联系的是密钥合法性字段，用来指示 PGP 信任“这是这个用户合法的公开密钥”的程度；信任程度越高，这个用户 ID 与这个密钥的绑定越紧密。这个字段由 PGP 计算。与每个实体相联系的还有用户收集的多个签名。反过来，每个签名都带有签名信任字段，用来指示该 PGP 用户信任签名者对这个公开密钥证明的程度。密钥合法性字段是从这个实体的一组签名信任字节中推导出来的。最后，每个实体定义了与特定的拥有者相联系的公开密钥，包括拥有者信任字段，用来指示这个公开密钥对其他公开密钥证书进行签名的信任程度(这个信任程度是由该用户指定的)。可以把签名信任字段看成是来自于其他实体的拥有者信任字段的副本。

总之，PGP 采用了 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法、加密前压缩等，以加密文件，还可以代替 Uuencode 生成 radix-64 格式(就是 MIME 的 BASE 64 格式)的编码文件。PGP 创造性地把 RSA 公钥体系的方便和传统加密体系的高速度结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计。这是目前最难破译的密码体系之一。

用户通过 PGP 的软件加密程序，可以在不安全的通信链路上创建安全的消息和通信。PGP 协议已经成为公钥加密技术和全球范围内消息安全性的事实标准。因为所有人都能看到它的源代码，从而查找出故障和安全性漏洞。

本 章 小 结

本章主要介绍了密码学的基本知识，包括：密码学的历史发展、密码学的含义和基本概

念；密码学的发展顺序中还介绍了古典密码学，其中包括凯撒密码、仿射密码以及 Playfair 密码和 Hill 密码等；结合当今的密码学现状介绍了对称密码算法和非对称加密体制，以及几种著名的加密算法，如 DES、AES、RSA 等以及这些算法在数字签名方面的应用，并且给出了相应算法的 Java 编程实例；最后讨论了有关 PGP 的相关内容和工作原理。希望读者通过本章的学习，能够掌握基础的密码学相关知识，为今后的网络安全防范打好基础。

课 后 练 习

一、 填空题

1. 在加密系统中，要加密的信息是(　　　　　)，经过变换加密后，成为(　　　　　)，这个变换的过程就称为(　　　　　)，通常由(　　　　　)来实现。

2. 在大多数的(　　　　　)算法中，加密和解密密钥是相同的，这些算法也叫做(　　　　　)。

3. 与传统密码体制相对应的是(　　　　　)，即公开密钥密码体制。加密密钥不同于解密密钥，加密密钥公之于众，而解密密钥只有解密人自己知道，这两个密钥分别称为(　　　　　)和(　　　　　)。

4. 公开密钥加密系统的一个优点是不仅可以用于信息的保密通讯，而且可以用来(　　　　　)和(　　　　　)。

5. 为了保证 RSA 密钥算法密码系统的安全性，最简明有效的做法就是不断增加(　　　　　)的位数。

二、 选择题

1. DES 算法将明文分为(　　)位的数据分组，使用(　　)位的密钥变换。

   A. 24　　B. 48　　C. 64　　D. 128

2. 下列密码算法，属于非对称性加密算法的是(　　)。

   A. 凯撒密码　　B. Vigenere 密码
   C. Playfair 密码　　D. RSA 算法

3. 以下密码算法，可以用于数字签名的是(　　)。

   A. DES/DSA　　B. Vigenere 密码
   C. Playfair 密码　　D. RSA 算法

4. PGP 采用了(　　)和传统加密的综合算法，用于数字签名的(　　)算法、加密前压缩等。

   A. AES　　B. DES　　C. RSA　　D. 邮件文摘

5. 分组密码算法通常由(　　)和(　　)两部分组成。

   A. 文件压缩算法　　B. 密钥扩展算法
   C. 加密/解密算法　　D. AES 算法

三、 简答题

1. 简述什么是“加密”，什么是“解密”。
2. 简述什么是对称密码算法，什么是非对称密码算法。
3. 相比之下，AES 算法比 DES 有什么优点?
4. 简述 RSA 算法的特点、安全性及其隐患。
5. 简述 PGP 的工作原理及优点。

第6章　身份认证与访问控制

身份认证技术是指计算机及网络系统确认操作者身份的过程中所应用的技术手段，通常是将某个身份与某个主体进行确认并绑定。访问控制机制按用户身份及其所归属的某预定义组限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制通过类似访问控制列表将控制访问的数据与客体进行绑定，能力表则将这种数据与主体进行绑定，用锁与钥匙在主体与客体之间分配这种数据。

本章重点

- 身份认证
- 访问控制
- 访问控制类型
- 访问控制机制

6.1　身 份 认 证

身份认证技术是在计算机网络中确认操作者身份的过程而产生的解决方法。计算机网络世界中一切信息(包括用户的身份信息)都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。如何保证以数字身份进行操作的操作者就是这个数字身份的合法拥有者，也就是说保证操作者的物理身份与数字身份相对应，身份认证技术就是为了解决这个问题，作为防护网络资产的第一道关口，身份认证有着举足轻重的作用。

6.1.1　身份认证概述

计算机系统和计算机网络是一个虚拟的数字世界。在这个数字世界中，一切信息包括用户的身份信息都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。而我们生活的现实世界是一个真实的物理世界，每个人都拥有独一无二的物理身份。如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，也就是说保证操作者的物理身份与数字身份相对应，就成为一个很重要的问题。

在真实世界中，验证一个人的身份主要通过三种方式判定：一是根据你所知道的信息来

证明你的身份(what you know)，假设某些信息只有某个人知道，比如暗号等，通过询问这个信息就可以确认这个人的身份；二是根据你所拥有的东西来证明你的身份(what you have)，假设某一个东西只有某个人有，比如印章等；三是直接根据你独一无二的身体特征来证明你的身份(who you are)，比如指纹、面貌等。

信息系统中，对用户的身份认证手段也大体可以分为这三种，仅通过一个条件的符合来证明一个人的身份称之为单因子认证，由于仅使用一种条件判断用户的身份容易被仿冒，我们可以通过组合两种不同条件来证明一个人的身份，称之为双因子认证。

身份认证技术从是否使用硬件可以分为软件认证和硬件认证，从认证需要验证的条件来看，可以分为单因子认证和双因子认证。从认证信息来看，可以分为静态认证和动态认证。身份认证技术的发展，经历了从软件认证到硬件认证，从单因子认证到双因子认证，从静态认证到动态认证的过程。

认证通常由两类实体组成：一类实体是用户，他们要向另一类实体证明自己的身份；另一类实体是验证者，他们要验证用户的身份。

6.1.2　常用的身份认证技术

1. 用户名/密码方式

用户名/密码是最简单也是最常用的身份认证方法，它是基于“what you know”的验证手段。每个用户的密码是由这个用户自己设定的，只有他自己才知道，因此只要能够正确输入密码，计算机就认为他就是这个用户。然而实际上，由于许多用户为了防止自己忘记密码，经常采用诸如自己或家人的生日、电话号码等容易被他人猜测到的有意义的字符串作为密码，或者把密码抄在一个自己认为安全的地方，这都存在着许多安全隐患，极易造成密码泄露。即使能保证用户密码不被泄漏，由于密码是静态的数据，并且在验证过程中需要在计算机内存和网络中传输，而每次验证过程使用的验证信息都是相同的，很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此用户名/密码方式是一种极不安全的身份认证方式，可以说基本上没有任何安全性可言。

2. IC 卡认证

IC 卡是一种内置集成电路的卡片，卡片中存有与用户身份相关的数据，IC 卡由专门的厂商通过专门的设备生产，可以认为是不可复制的硬件。IC 卡由合法用户随身携带，登录时必须将 IC 卡插入专用的读卡器读取其中的信息，以验证用户的身份。IC 卡认证是基于“what you have”的手段，通过 IC 卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从 IC 卡中读取的数据还是静态的，通过内存扫描或网络监听等技术很容易截取到用户的身份验证信息。因此，静态验证的方式还是存在根本的安全隐患。

3. 生物特征认证

生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术，常见的有指纹识别、虹膜识别等。从理论上说，生物特征认证是最可靠的身份认证方式，因为它直接使

用人的物理特征来表示每一个人的数字身份，不同的人具有相同生物特征的可能性可以忽略不计，因此几乎不可能被仿冒。

生物特征认证基于生物特征识别技术，受到现在的生物特征识别技术成熟度的影响，采用生物特征认证还具有较大的局限性。首先，生物特征识别的准确性和稳定性还有待提高，特别是如果用户身体受到伤病或污渍的影响，往往导致无法正常识别，造成合法用户无法登录的情况。其次，由于研发投入较大和产量较小的原因，生物特征认证系统的成本非常高，目前只适合于一些安全性要求非常高的场合(如银行、部队等)使用，还无法做到大面积推广。

4. USB Key 认证

基于 USB Key 的身份认证方式是近几年发展起来的一种方便、安全、经济的身份认证技术，它采用软硬件相结合一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB Key 内置的密码学算法实现对用户身份的认证。基于 USB Key 身份认证系统主要有两种应用模式：一种是基于冲击/相应的认证模式，另一种是基于 PKI 体系的认证模式。

5. 动态口令/动态密码

动态口令技术是一种让用户的密码按照时间或使用次数不断动态变化，每个密码只使用一次的技术。它采用一种称之为动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份的确认。由于每次使用的密码必须由动态令牌来产生，只有合法用户才持有该硬件，所以只要密码验证通过就可以认为该用户的身份是可靠的。而用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

动态口令技术采用一次一密的方法，有效保证了用户身份的安全性。

6. 数字签名

数字签名又称电子加密，可以区分真实数据与伪造、被篡改过的数据。这对于网络数据传输，特别是电子商务极其重要，一般要采用一种被称为摘要的技术，摘要技术主要采用 HASH(哈希)函数。HASH 函数提供了这样一种计算过程：输入一个长度不固定的字符串，返回一串定长度的字符串，又称 HASH 值，将一段长的报文通过函数变换，转换为一段定长的报文，即摘要。身份识别是指用户向系统出示自己身份证明的过程，主要使用约定口令、智能卡和用户指纹、视网膜和声音等生理特征。数字证明机制提供利用公开密钥进行验证的方法。

6.1.3　常用的身份认证机制

下面讨论几种常用的身份认证机制，并对它们的安全性进行分析。

1. RADIUS 认证机制

RADIUS(Remote Authentication Dial In User Service)协议最初是由 Livingston 公司提出的，原先的目的是为拨号用户进行认证和计费。后来经过多次改进，形成了一项通用的认证计费协议。RADIUS 认证要用到基于挑战/应答(Challenge/Response)的认证方式。

RADIUS 是一种 C/S 结构的协议，它的客户端最初就是 NAS(Net Access Server)，现在任何运行 RADIUS 客户端软件的计算机都可以成为 RADIUS 的客户端。RADIUS 协议认证机制灵活，可以采用 PAP、CHAP 或者 Unix 登录认证等多种方式。RADIUS 是一种可扩展的协议，它进行的全部工作都是基于 Attribute-Length-Value 的向量进行的。

RADIUS 的基本工作原理是用户接入 NAS，NAS 向 RADIUS 服务器使用 Access-Require 数据包提交用户信息，包括用户名、密码等相关信息，其中用户密码是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播；RADIUS 服务器对用户名和密码的合法性进行检验，必要时可以提出一个 Challenge，要求进一步对用户认证，也可以对 NAS 进行类似的认证；如果合法，给 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作，否则返回 Access-Reject 数据包，拒绝用户访问；如果允许访问，NAS 向 RADIUS 服务器提出计费请求 Account-Require，RADIUS 服务器响应 Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。

RADIUS 服务器和 NAS 服务器通过 UDP 协议进行通信，RADIUS 服务器的 1812 端口负责认证，1813 端口负责计费工作。采用 UDP 的基本考虑是因为 NAS 和 RADIUS 服务器大多在同一个局域网中，使用 UDP 更加快捷方便。

RADIUS 协议还规定了重传机制。如果 NAS 向某个 RADIUS 服务器提交请求没有收到返回信息，那么可以要求备份 RADIUS 服务器重传。由于有多个备份 RADIUS 服务器，因此 NAS 进行重传的时候，可以采用轮询的方法。如果备份 RADIUS 服务器的密钥和以前 RADIUS 服务器的密钥不同，则需要重新进行认证。

RADIUS 协议应用范围很广，包括普通电话、上网业务计费，对 VPN 的支持可以使不同的拨入服务器的用户具有不同的权限。

2. 基于 DCE/Kerberos 的认证机制

DCE/Kerberos 是一种被证明为非常安全的双向身份认证技术。DCE/Kerberos 的身份认证强调了客户机对服务器的认证；而其他产品只解决了服务器对客户机的认证。

下面简要介绍 DCE/Kerberos 的身份认证的形式化过程。

1) 形式化过程涉及的元素

在开始之前，首先要对过程中涉及的元素做一个定义，具体如下。

K：密钥。

A：身份认证服务器。

C：用户。

P：访问授权服务器。

PAC：访问授权服务器签发的授权凭证。

S：应用服务器，如 Web 服务器、数据库服务器等。

{…}K_n：表示用 K_n 加密大括号中的内容。

2) DCE/Kerberos 的身份认证的形式化过程

DCE/Kerberos 的身份认证的形式化过程大致有如下几个步骤。

第一步：用户 C 从身份认证服务器 A 获得通信凭据{K,C}K_a，该凭证可以理解为由身份认证服务器签发的一次性电子身份证或电子护照。

第二步：用户 C 使用第一步得到的凭据{K_1,C}K_a 申请访问授权服务器 P 的通信凭据{K_2,C}K_p，该凭证可以理解为身份认证服务器为用户签发了访问授权服务器的电子介绍信。

第三步：用户向授权服务器 P 申请授权凭证 PAC。授权服务器根据身份认证服务器签发的电子介绍信，为该用户签发一次性的出境许可。

第四步：用户申请能够向服务器 S 证实自己身份、并得到授权许可的凭证{PAC, K_4}K_s，该凭证可以理解为应用服务器为该用户签发了一次性的入境签证。

第五步：用户 C 获得与应用服务器 S 通信的密钥 K5，该密钥可以理解为应用服务器为用户签发了一次性的境内通行证。

3. 基于公共密钥的认证机制

目前在 Internet 上也使用基于公共密钥的安全策略进行身份认证，具体而言，就是使用符合 X.509 的身份证明。使用这种方法必须有一个第三方的证明授权(CA)中心为客户签发身份证明。客户和服务器各自从 CA 获取证明，并且信任该证明授权中心。

在会话和通讯时首先交换身份证明，其中包含了将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名、交换通讯的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认该证明是否有效，如图 6-1 所示。

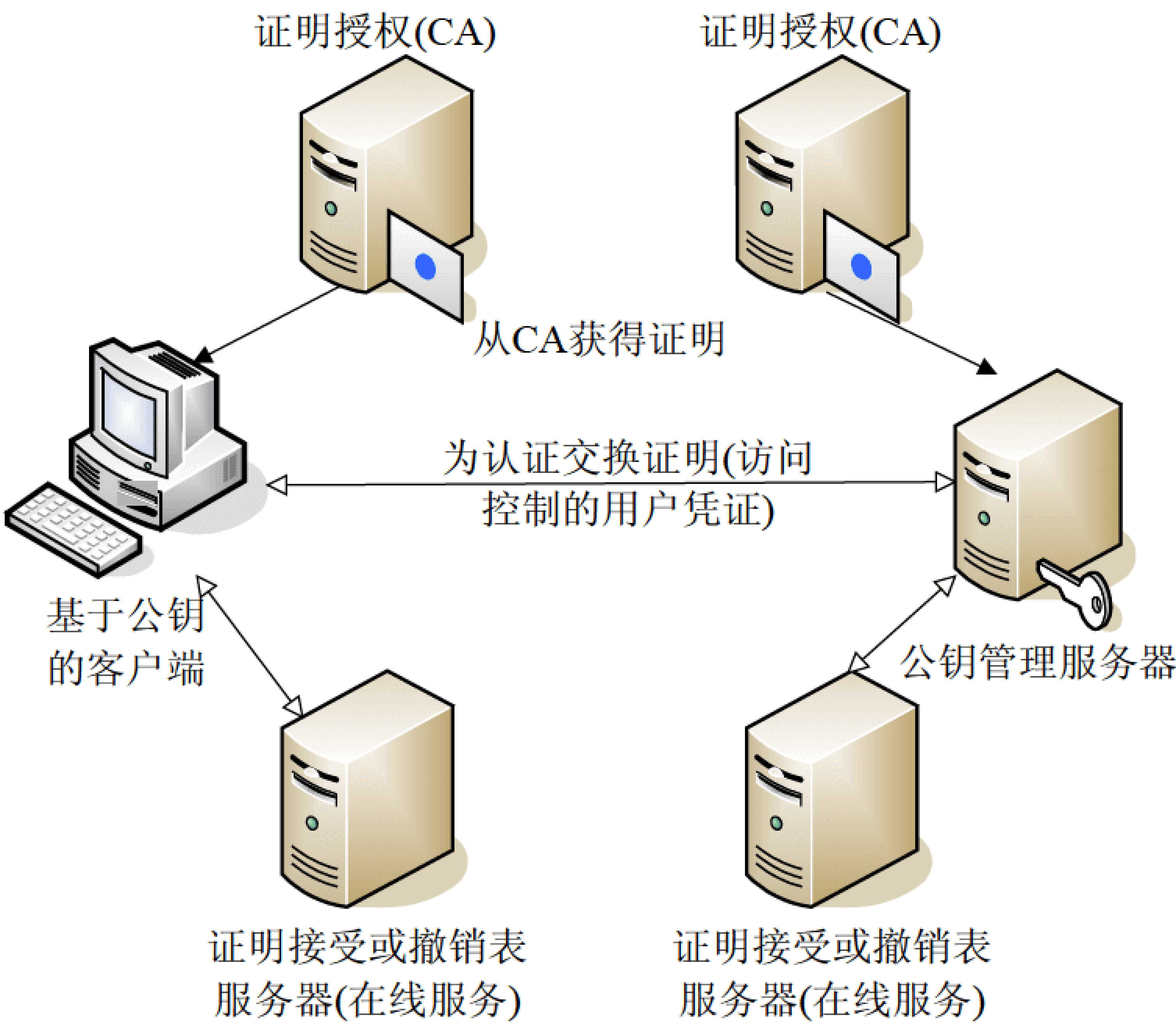


图 6-1　基于公共密钥的认证系统

在一般的实现机制中，常将基于公共密钥的 SSL 策略集成在一起，多用在 Web 应用方

面。认证服务器通过公共密钥管理服务器(PKMS)与 SSL 连接起来。PKMS 实际是身份认证网关和建立基于 SSL 的加密通道，客户端不必使用客户端软件，可使用 SSL 浏览器登录到 PKMS，PKMS 将用户的身份映射成系统用户身份并且通过 RPC 进行传输，也就是将 SSL 的用户标识传递给认证服务器。PKMS 用来与 Internet 用户之间临时建立起相互信任的安全会话过程，然后将 Internet 用户身份映射到系统访问控制机制可以管理的用户身份，如图 6-2 所示。

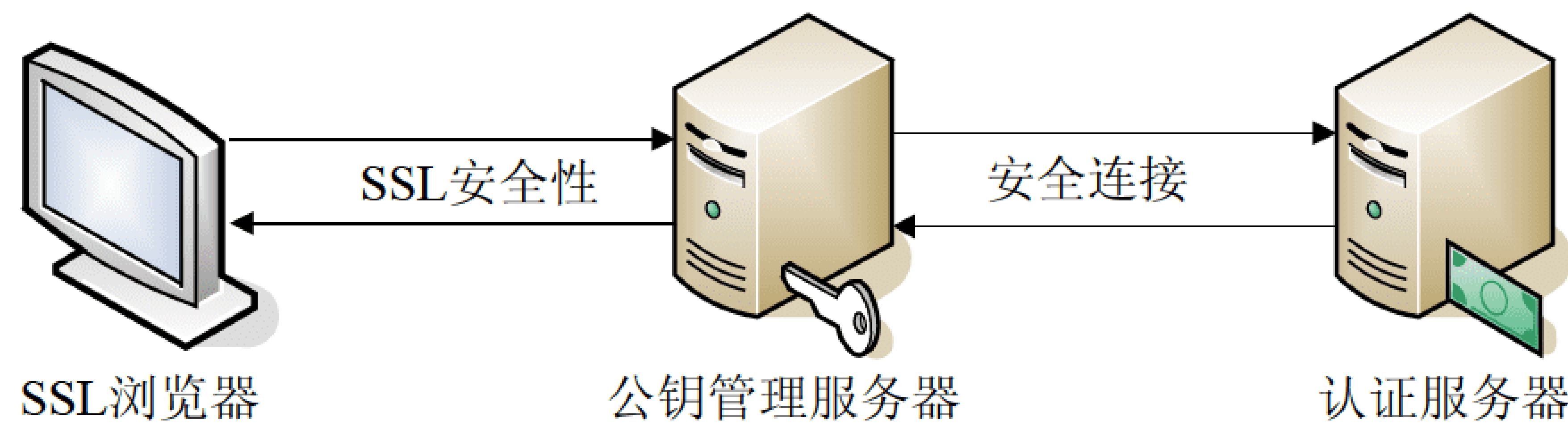


图 6-2　SSL 浏览器、PKMS、认证服务器的交互

基于公共密钥的认证过程如下。

在 PKMS 和使用支持 SSL、S-HTTP 的浏览器用户之间的身份验证是建立在公开密钥加密数字签名和授权证明之上的。数字签名工作为：用户产生一段文字信息，然后对这段文字信息进行单向不可逆的变换。用户再用自己的秘密密钥对生成的文字变换进行加密，并将原始的文字信息和加密后的文字变换结果传送给指定的接收者。这段经过加密的文字变换结果就被称作数字签名。

文字信息和加密后的文字变换的接收者将收到的文字信息进行同样的单项不可逆的变换。同时也用发送方的公开密钥对加密的文字变换进行解密。如果解密后的文字变换和接收方自己产生的文字变换一致，接收方就可以相信对方的身份，因为只有发送方的秘密密钥能够产生加密后的文字变换。

要向发送方验证接收方的身份，接收方根据自己的密钥创建一个新的数字签名，然后重复上述过程。

一旦两个用户互相验证了身份，他们就可以交换用来加密数据的密钥(如 DES 加密密钥)。公开密钥加密方法对于大量的数据加密来说速度太慢。浏览器应该能够在类似的交换过程使用它的公开/秘密密钥组合对来验证它的身份。但是目前还没有出现支持浏览器身份验证的产品。

为了利用数字签名，接收方必须拥有发送方的公开密钥。公开密钥是通过授权证明(Certificates of Authority，CA)来发布的。PKMS 把它的经公开密钥加密的 CA 发送给浏览器。多数公钥产品只使用了服务器方的身份验证，所以在 CA 中只需要包含 PKMS 的公开密钥，这些授权证明是由可信赖的第三方生成的并且经过可信赖的第三方用秘密密钥“数字签名”的。

用户的浏览器(或者其他客户方的程序)要接收由受信赖的第三方签发的正确的 CA 就必须要配置受信赖的第三方的公开密钥。浏览器用户使用配置好受信赖的第三方公开密钥的浏览器来验证 CA 中的受信赖的第三方的数字签名。如果该浏览器没有配置受信赖的第三方的公开密钥，它就无法验证安全网关的身份。一些浏览器预先配置有受信赖的第三方公开密钥，并且用户不能增加其他的签发 CA 的受信赖的第三方。这限制了将无关公司推出的浏览器的

用户与公司拥有的服务器之间建立相互信任关系的能力。

基于 DCE/Kerberos 和公共密钥的用户身份认证是非常安全的用户认证形式，但是，它们实现起来比较复杂，要求通信的次数多，而且计算量较大。

4. 基于挑战/应答的认证机制

顾名思义，基于挑战/应答(Challenge/Response)方式的身份认证机制就是每次认证时认证服务器端都给客户端发送一个不同的“挑战”字串，客户端程序收到这个“挑战”字串后，做出相应的“应答”。

1) 认证过程

一个典型的认证过程如图 6-3 所示。

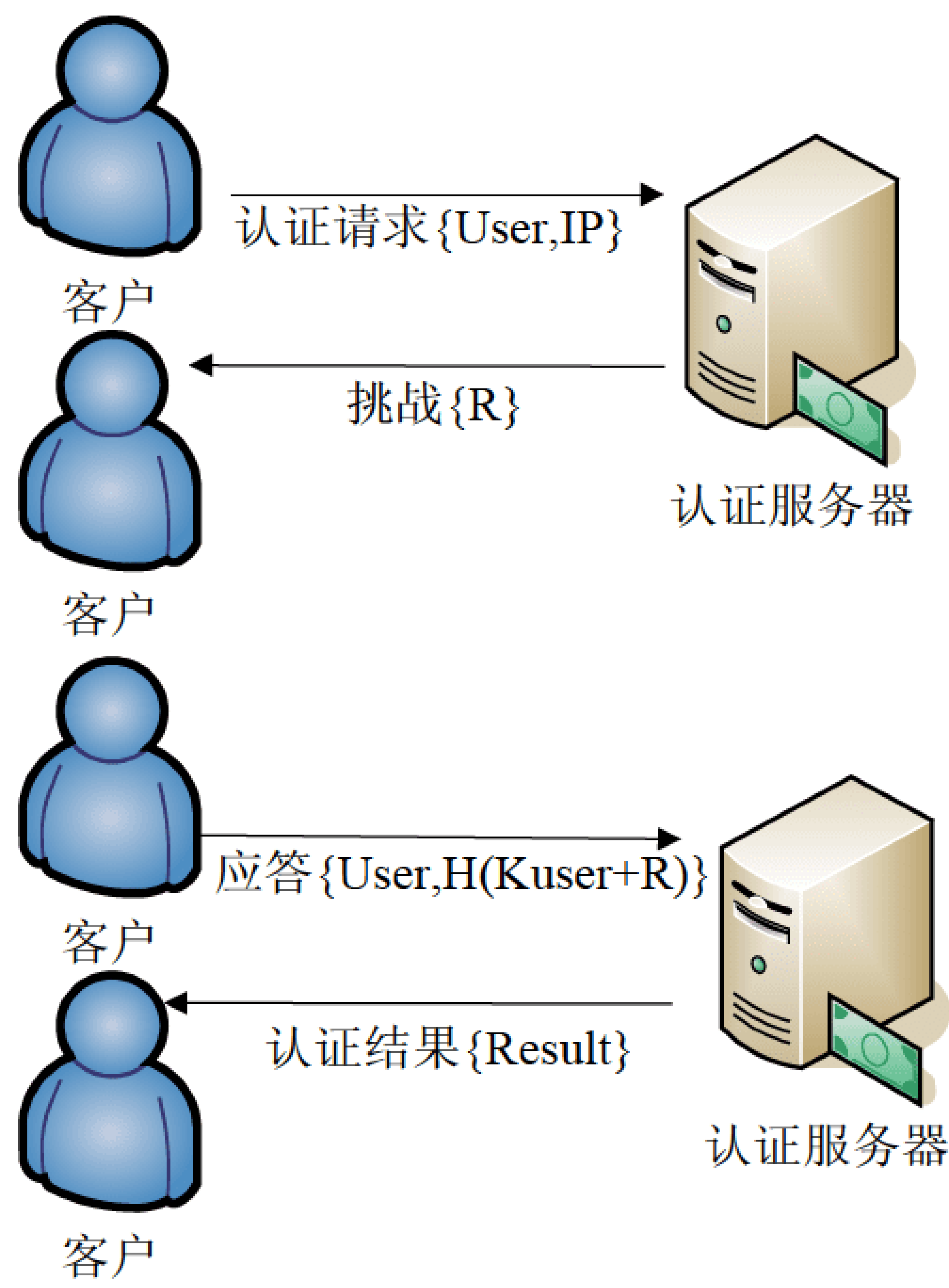


图 6-3　客户认证过程

图中的 R 代表 32 位的随机数；H 代表单向的 HASH 函数；Kuser 代表用户的密钥。

认证过程如下。

(1) 客户向认证服务器发出请求，要求进行身份认证。

(2) 认证服务器从用户数据库中查询用户是否是合法的用户，若不是，则不做进一步处理。

(3) 认证服务器内部产生一个随机数，作为“提问”发送给客户。

(4) 客户将用户名字和随机数合并，使用单向 Hash 函数(例如 MD5 算法)生成一个字节串作为应答。

(5) 认证服务器将应答串与自己的计算结果比较，若二者相同，则通过一次认证；否则，认证失败。

(6) 认证服务器通知客户认证成功或失败。

以后的认证由客户不定时地发起，过程中没有了客户认证请求一步。两次认证的时间间隔不能太短，否则就给网络、客户和认证服务器带来太大的开销；也不能太长，否则不能保证用户不被他人盗用 IP 地址，一般定为 1~2 分钟。

2) 密钥的分配和管理

密钥的分配由维护模块负责，当用户注册时，自行设定自己的口令字。用户的密钥由口令字生成。

一个口令字必须经过两次口令字检查。第一次由注册程序检查，强制口令字必须有足够的长度(如 8 个字符)。口令字被加密后送入数据库中，这个口令字标记为“未检查的”。第二次由离线的口令字检查工具进行检查，将弱口令字进行标记，当下一次用户认证时，认证服务器将强制用户修改口令字。密钥的在线修改由认证服务器完成，它的过程与认证过程基本类似。

需要说明的是，每种认证机制都不是绝对的，它们之间有些方式都是类似的，实际选择的时候有可能会结合两种或两种以上的认证技术。随着 Internet 技术尤其是网络安全技术的发展，必将涌现出更多更好的用户认证机制。

6.2　访 问 控 制

随着互联网的发展，随之而来的就是计算机资源所面临的一大难题：计算机数据安全管理。在国际标准化组织(ISO)对计算机安全标准(ISO7498—2)定义的五个层次安全服务中，访问控制是其中一个重要的组成部分。计算机安全的根本所在就是控制信息资源如何被用户访问，因此访问控制技术是一项非常重要的安全手段，它控制用户与系统之间以及其他系统之间的通信和交互。

6.2.1　访问控制概述

访问控制技术可以限制对计算机关键资源的访问，防止非法用户进入系统和合法用户对系统资源的非法使用。访问控制的手段包括用户识别代码、口令、登录控制、资源授权(例如用户配置文件、资源配置文件和控制列表)、授权核查、日志和审计。到目前为止，访问控制已经深入到了计算机系统的各个层面与细节。举个例子，比方当用户需要使用计算机时，系统要求用户输入用户名和口令，这就是一种访问控制，可以确保合法用户正确地使用计算机；当访问外部网络的资源时，防火墙将验证用户的访问是否被允许，这也是一种形式的访问控制。

6.2.2　访问控制的基本要素

访问控制技术的目标是防止对任何资源(如计算机资源、通信资源或者信息资源等)进行未授权访问，从而使计算机系统在合法范围内被使用；决定用户能做什么，也决定代表一定用户权益的程序能做什么。未授权的访问是指未经授权的使用、泄露、修改、销毁信息以及发送指令等，非法用户进入系统，或合法用户对系统资源的非法使用。总而言之，访问控制是给予组织控制、限制、监控以及保护资源的可用性、完整性和机密性的一种能力。

1) 访问控制的主要目标

访问控制的主要目标包括如下方面。

- 机密性要求：保证信息不被泄露给非授权的人或者实体。

- 完整性要求：保证数据的一致性，防止数据被非授权建立、修改和破坏。
- 可审计性：对非法用户的入侵行为、信息的泄露与破坏的情况能够跟踪审计。
- 可用性：保证授权用户对系统信息的可访问性。

2) 访问控制的基本要素

访问控制是指主体根据某些控制策略或权限对客体本身或是其资源进行的不同的授权访问。访问控制包括三个要素：主体、客体和控制策略。

- 主体(Subject)：是一个主动的实体，是访问的发起者，但不一定是访问的执行者，我们标识为 S。
- 客体(Object)：是接受主体或主体发动的对象进行访问的被动实体，我们标识为 O。
- 控制策略：是主体对客体的操作行为集合和约束条件集合，标识为 KS，通常用 P 表示。

3) 访问控制的实现

访问控制系统的三个要素之间可以用三元组(S、O、P)来表示(主体、客体、许可)，当主体 S 提出正常的请求信息时，信息系统的 KS 监控器判断是否允许或拒绝请求，即对主体进行认证，主体通过 KS 监控器的验证才能访问客体。访问控制的过程主要包括认证、控制策略的具体实现和审计三个方面的内容。

- 认证：包括主体对客体的识别认证和客体对主体检验认证。
- 控制策略的具体实现：指设定规则集合应该确保正常用户对信息资源的合法使用。
- 审计：因为客体的管理者(即管理员)有操作赋予权，有可能滥用这种权利，这是在策略中无法加以约束的，因此必须对这些行为进行记录，从而达到监督和保证访问控制正常实现的目的，这就是审计的重要意义。

6.3　访问控制类型

访问控制机制可以限制对关键资源的访问，防止非法用户进入系统，以及合法用户对系统资源的非法使用。目前的主流访问控制技术有：自主访问控制(Discretionary Access Control Model，DAC)、强制访问控制(Mandatory Access Control Model，MAC)、基于角色的访问控制(Role Based Access Control，RBAC)。

6.3.1　自主型访问控制(DAC)

自主访问控制模型也称为基于身份的访问控制(IBAC)，是针对访问资源的用户或应用位置访问控制权限，根据主体的身份及允许访问的权限进行决策。自主是指具有某种访问能力的主体能够自主地将访问权的某个子集授予其他主体。

自主访问控制可以分为以下两类。

- 基于个人的策略：根据哪些用户可对一个目标实施哪一种行为的列表来表示，等于用一个目标的访问矩阵的列来描述。

- 基于组的策略：一组用户对于一个目标具有同样的访问许可，是基于身份策略的另一种情形，相当于把访问矩阵中的多个行压缩为一个列。实际使用时，应先定义组的成员，对用户组授权，同一个组可以被重复使用。可以改变组的成员。

自主访问控制的特点是灵活性高，可被大量采用；缺点是：安全性低。自主访问控制存在的问题是配置的粒度小，配置的工作量大，效率有些低。

6.3.2　强制型访问控制(MAC)

强制访问控制(MAC)也称为基于规则的访问规则。强制访问控制在自主访问控制的基础上，增加了对资源的属性(安全属性)划分，规定不同属性下的访问权限。强制访问控制模型最初是为了实现比自主访问控制更加严格的访问控制策略，美国政府和军方开发了各种各样的强制访问控制模型，这些方案或模型都有比较完善和详尽的定义。随后，逐渐形成强制访问的模型，并得到广泛的关注和应用。在自主访问控制中，用户和客体资源都被赋予一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限。

自主访问控制技术有一个最主要的缺点：不能有效地抵抗计算机病毒的攻击，在自主访问控制技术中，某一合法用户可以任意运行一段程序来修改该用户拥有的文件访问控制信息，而操作系统无法区别这种修改是用户自己的合法操作还是计算机病毒的非法操作；另外，也无法防止计算机病毒将信息通过共享客体(文件、内存等)从一个进程传给另一个进程。

在强制访问控制中，系统对主体与客体都分配一个特殊的一般不能更改的安全属性，系统通过比较主体与客体的安全属性来决定一个主体是否能够访问某个客体。用户为某个目的而运行的程序不能改变它自己及任何其他客体的安全属性，包括该用户自己拥有的客体。强制访问控制还可以阻止某个进程生成共享文件并通过这个共享文件向其他进程传递信息。

6.3.3　基于角色的访问控制(RBAC)

美国 George Mason 大学信息系统和系统工程系的 R.Sandhu 等人在对 RBAC(基于角色的访问控制)进行深入研究的基础上，于 1996 年提出了一个基于角色的访问控制参考模型(RBAC96 模型)，该模型对角色访问控制产生了重要影响。同年，George Mason 大学的 Ravi 等人提出了 RBAC96 的基础模型 RBAC0、高级模型 RBAC1、约束模型 RBAC2 和组合模型 RBAC3。

由于 RBAC96 模型全面、系统地描述了 RBAC 多方面、多层次的意义，从而得到了广泛的认可。RBAC96 模型包括 4 个不同层次，分别为 RBAC0 、RBAC1、 RBAC2、 RBAC3。其中，RBAC0 是基础模型，定义了支持 RBAC 的最小需求，如用户、角色、权限、会话等概念。RBAC1 和 RBAC2(高级模型)在 RBAC0 的基础上，又加上了各自独立的特点。在 RBAC1 中加入了角色继承关系，可以根据组织内部权力和责任的结构来构造角色与角色之间的层次关系：在 RBAC2 中加入了各种用户与角色之间、权限与角色之间以及角色与角色之间的约束关系，如角色互斥、角色最大成员数等。RBAC1 和 RBAC2 之间不具有可比性。RBAC3(组合模型)是对 RBAC1 和 RBAC2 的集成，它不仅包括角色的层次关系，还包括约束关系。RBAC96 模型间的关系如图 6-4 所示。

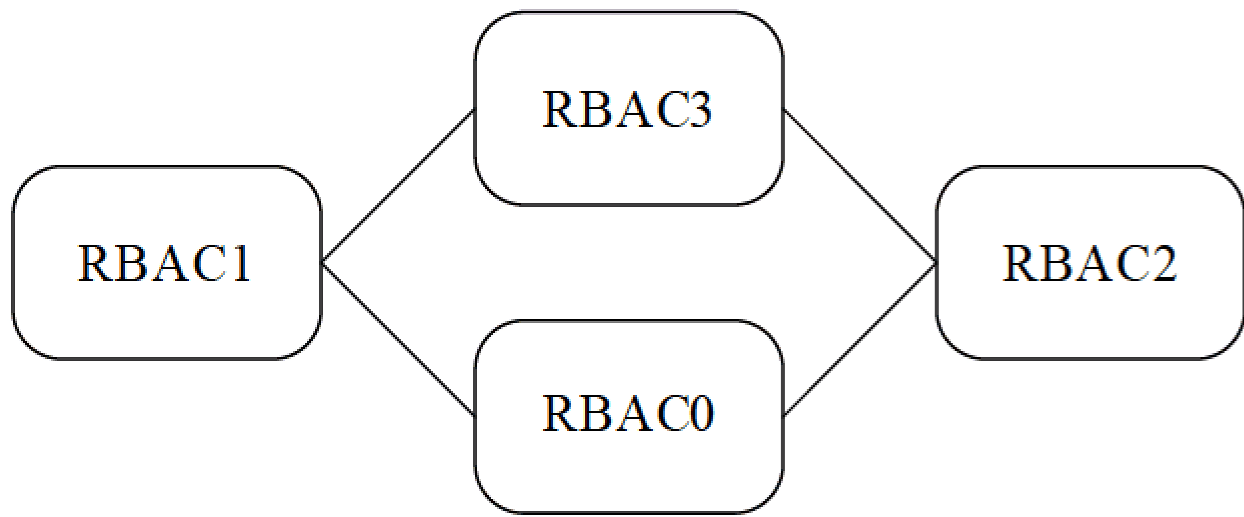


图 6-4　RBAC96 模型间的关系

RBAC 模型的基本思路是在用户和访问许可权之间引入角色(Role)的概念，用户与特定的一个或多个角色相联系，角色与一个或多个访问许可权相联系，角色可以根据实际的工作需要生成或取消，而用户可以根据自己的需要动态地激活自己拥有的角色，从而避免了用户无意中危害系统安全。RBAC 技术由于其对角色和层次化管理的引进，特别适用于用户数量庞大、系统功能不断扩展的大型系统。

通常，实现 RBAC 模型的基本原则如下所述。

- 角色继承项目。
- 最小权限原则。最小权限原则是指用户所拥有的权力不能超过他执行工作时所需的权限。
- 职责分离原则。对于某些特定的操作集，某一个角色或用户不可能同时独立地完成所有这些操作。

6.4　访问控制机制

6.4.1　访问控制列表

访问控制列表(Access Control List，ACL)可以决定任何一个特定的主体是否可以对某一个客体进行访问。它是利用在客体上附加一个主体明细表的方式来表示访问控制的矩阵。表中的每一项包括主体的身份以及对该客体的访问权。

该表通常包含有此文件的用户身份、文件属主、用户组，以及文件属主或用户组成员对此文件的访问权限。

6.4.2　能力机制

能力(Capabilities)决定用户对客体的访问权限(读、写、执行)，在这种机制下，系统必须对每个用户维护一份能力表，表中存有该用户对系统中各目标客体的访问权限信息。在用户较少的系统中，这种方式比较好。但是一旦用户数目增加，便要花费大量的时间和系统资源来维护每个用户的能力表，这种资源上的消耗必然成为系统设计者需要考虑的因素之一。

6.4.3　安全标签机制

另一种机制是采用某种特殊标签，例如前缀，包含受保护的客体名及主体对它的访问权限。当系统中某个主体需要访问某个客体时，访问控制机制将检查主体的前缀里是否具有它所请求的访问权。这种方式有三个问题需要考虑：前缀大小的限制；当生成一个新的客体或者改变某个客体的访问权时，如何对主体分配访问权；如何决定可访问某个客体的所有主体。由于客体名通常是杂乱无章的，所以很难进行分类，而且当一个主体可以访问多个客体时，它的前缀也将非常大，这样也很难于管理。另外，受保护的客体必须具有唯一的名字，互相不能重名，因此造成客体名的数目庞大。此外，在进行客体创建撤销动作或变更访问权限时，可能会涉及许多主体前缀的更新，因此需要进行的操作比较多。

本 章 小 结

本章主要介绍了身份认证和访问控制的基本知识，包括：身份认证的概念；常用身份认证技术和机制(对几种用户认证机制：RADIUS 认证、基于 DCE/Kerberos 的认证、基于公共密钥的认证、基于挑战/应答的认证机制进行了剖析)；访问控制的原理和基本要素；访问控制的几种基本类型(DAC、MAC 和 RBAC)，以及常见的几种访问控制机制进行了阐述，希望读者通过本章的学习能够掌握基础的身份认证和访问控制相关知识。

课 后 练 习

一、 填空题

1. 常用的身份认证技术主要有(　　　　　)、(　　　　　)、(　　　　　)、(　　　　　)、(　　　　　)。
2. RADIUS 是一种(　　　　　)结构的协议，它的客户端最初是(　　　　　)，认证机制灵活，可以采用 PAP、CHAP 或(　　　　　)等多种方式。
3. DCE/Kerberos 是一种被证明为非常安全的(　　　　　)认证技术。
4. 访问控制的主要目标包括机密性要求、(　　　　　)、(　　　　　)、(　　　　　)。
5. 目前的主流访问控制技术有(　　　　　)、(　　　　　)、(　　　　　)。

二、 选择题

1. 以下口令中，(　　)好口令，(　　)是坏口令。
   A. Mary　　B. ga2work　　C. cat&dog　　D. 3.1515pi
2. 以下认证技术中，属于身份认证范畴的是(　　)。
   A. IC 卡认证　　B. 生物特征认证
   C. USB KEY 认证　　D. 动态口令/动态密码
3. 目前的主流访问控制技术有(　　)。
   A. 基于角色的访问控制　　B. 强制访问控制
   C. 自主访问控制　　D. Kerberos
4. 验证一个人身份的手段大体可以分为三种，包括(　　)。
   A. what you know　　B. what you have
   C. what is your name　　D. who are you
5. 现实生活中我们遇到的短信密码确认方式，属于(　　)。
   A. 动态口令牌　　B. 电子签名　　C. 静态密码　　D. 动态密码

三、 简答题

1. 简单列举现实生活中运用 IC 卡认证技术的场合，说明此种方式的优点和不足。
2. 简单描述基于公钥密码的认证体制的主要原理。
3. 访问控制主要包括哪几个要素？它们之间的关系是什么？
4. 自主访问控制可以分成哪两类？该机制存在的问题是什么？
5. 浅谈生物特征认证技术的优缺点。

第7章　数据库安全

随着计算机及网络应用的全面普及，数据库和数据库技术在各行各业都起着至关重要的作用。没有数据库的安全和保护，计算机和网络应用的深度和广度都将受到很大的影响。与系统的安全性相比，数据库的安全性往往容易被忽视，许多管理员错误地认为只要把网络和操作系统的安全搞好了，所有的应用程序也就安全了。事实上，数据库系统中存在的安全问题同样会造成严重的后果，研究数据库安全问题具有重要价值。

本章重点

- 数据库系统的三种安全机制
- 存取控制模型的分类、概念
- 数据完整性分类及概念
- 数据库系统备份模式及相关的恢复手段
- SQL Server 数据的身份验证和访问控制机制

7.1　数据库安全概述

7.1.1　数据库简介

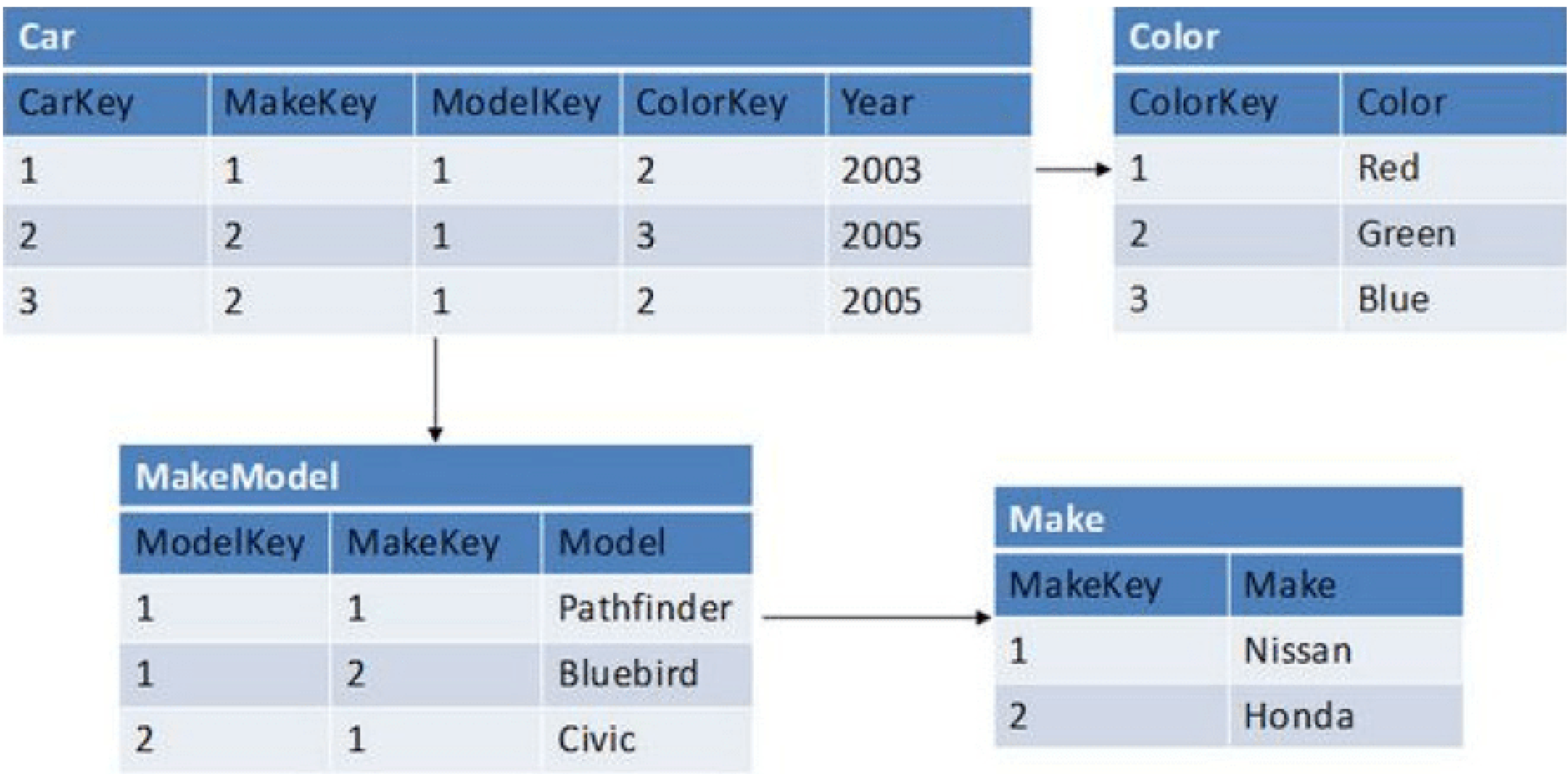
数据库(Database，DB)是指长期保存在计算机的存储设备上，并按照某种模型组织起来的，可以被各种用户或应用共享的数据的集合。数据库管理系统(Database Management System，DBMS)是指提供各种数据管理服务的计算机软件系统。DBMS 提供的服务包括：数据对象定义、数据存储与备份、数据访问与更新、数据统计与分析、数据安全保护、数据库运行管理以及数据库的建立和维护等。各行各业信息化的目的就是要以现代信息技术为手段，对企业生产和经营过程产生的数据进行收集、加工、管理和利用，以改善生产经营的整体效率，增强企业的竞争力。因此，数据库是各行各业信息化不可缺少的工具，是绝大部分企业信息系统的核心。

数据库技术从 20 世纪 60 年代中期产生，其发展速度之快、应用范围之广令人惊叹。数据库技术的研究和发展已成为现代信息化社会具有强大生命力的一个重要领域。数据库技术已经取得了辉煌的成就，发展成为一门内容丰富的学科，形成了总量达数百亿美元的一个软件产业。根据 Gartner Dataquest(美国高德纳，全球最具权威的 IT 研究与顾问咨询公司之一)

公司的调查，2005 年国际数据库市场销售总额达 1600 亿美元。数据库已经发展成为一个规模巨大、增长迅速的市场。目前，市场上具有代表性的数据库产品包括 Oracle 公司的 Oracle、IBM 公司的 DB2 以及微软的 SQL Server 等。这些产品的特征很大程度上反映了当前数据库产业界的最高水平和发展趋势。

目前成熟地应用在数据库系统中的数据模型有：层次模型、网状模型和关系模型。其中，层次模型和网状模型是非关系模型，层次模型数据库系统和网状模型数据库系统统称为第一代数据库系统，关系型数据库管理系统(Relational Database Management System，RDBMS)称为第二代数据库系统。20 世纪 70 年代至 80 年代初，层次模型数据库系统和网状模型数据库系统很流行，现在逐步被关系模型取代。关系数据库技术出现在 20 世纪 70 年代，经过 80 年代的发展到 90 年代已经比较成熟，在 90 年代初期曾一度受到面向对象数据库的挑战，但市场最后还是选择了关系数据库。到目前为止，数据库技术的研究与应用绝大多数以关系数据库为基础，无论是 Oracle 公司的 Oracle、IBM 公司的 DB2，还是微软的 SQL Server 等都是关系型数据库。Gartner Dataquest 的报告显示关系数据库管理系统的市场份额最大，2005 年 RDBMS 的市场份额增幅达 9.4%。当前，由于互联网应用的兴起，XML 格式的数据大量出现，支持 XML 模型的新型数据库成为需求，但是关系数据库技术仍然是主流，无论是多媒体内容管理、XML 数据支持还是复杂对象支持等，都将是在关系数据库系统内核技术基础上的扩展。

典型的关系数据库示例如图 7-1 所示。图中有 Car、Color、MakeModel、Make 四个数据表(Table)，四个表之间通过相关字段(Filed)建立起关系，故称之为关系数据库。例如表 Car 和表 Color 之间通过 ColorKey 字段建立关系，表 Car 和表 MakeModel 之间通过 ModelKey 字段建立关系。



Car

CarKey	MakeKey	ModelKey	ColorKey	Year
1	1	1	2	2003
2	2	1	3	2005
3	2	1	2	2005

Color

ColorKey	Color
1	Red
2	Green
3	Blue

MakeModel

ModelKey	MakeKey	Model
1	1	Pathfinder
1	2	Bluebird
2	1	Civic

Make

MakeKey	Make
1	Nissan
2	Honda

图 7-1　典型的关系数据库模型

在关系数据库保持着占据数据库市场主流地位的同时，当前数据库系统发展还有以下几个特点。

1. 数据库产品系列化

一方面，Web 和数据仓库等应用的兴起，数据的绝对量在以惊人的速度迅速膨胀。另一方面，移动和嵌入式应用快速增长，使得针对市场的不同需求，数据库正在朝系列化方向发

展。例如，IBM 公司的 DB2 通用数据库产品包括了从高端的企业级并行数据库系统，到移动端产品 DB2 Everywhere 的一整套系列产品。从支持平台看，今天的 DB2 已经不再是大型机上的专有产品，它支持目前主流的各种平台，包括 Linux 和 Windows。此外，它还有各种中间件产品，如 DB2 Connect、DB2 Datajointer、DB2 Replication 等，构成了一个庞大的数据库家族。

2. 支持各种互联网应用

数据库管理系统是网络经济的重要基础设施之一。支持 Internet 的数据库应用已经成为数据库系统的重要特征。例如，Oracle 公司的产品从其 8.0 版起全面支持互联网应用，是互联网数据库的典型代表。微软公司更是将 SQL Server 作为其整个.NET 计划中的一个重要环节。对于互联网应用，由于用户数量是无法事先预测的，这就要求数据库系统比以前拥有处理更大量的数据，以及为更多的用户提供服务的能力，也就是要拥有良好的可伸缩性及高可用性。此外，互联网提供大量以 XML 格式数据为特征的半结构化数据，支持这种类型的数据的存储、共享、管理、检索等也是各数据库厂商的发展方向。

3. 智能化、集成化

数据库技术的广泛使用为企业和组织收集并积累了大量的数据。数据丰富、知识贫乏的现实直接导致了联机分析处理(On-Line Analytical Processing，OLAP)、数据仓库(Data Warehousing，DW)和数据挖掘(Data Mining，DM)等技术的出现，促使数据库向智能化方向发展。同时企业应用越来越复杂，涉及应用服务器、Web 服务器、其他数据库系统、旧系统中的应用以及第三方软件等。数据库产品与这些软件是否具有良好集成性往往关系到整个系统的性能。Oracle 公司的 Oracle 9i 产品包括了 OLAP、DM、ETL(Extract-Transform-Load，数据抽取、转换、装载)工具等一套完整的商业智能支持平台。并且中间件产品与其核心数据库具有紧密集成的特性，Oracle Application Server 增加的一项关键功能是高速缓存特性，该特性可以将数据从数据库迁移至应用服务器，加速 Web 用户对数据的访问速度。IBM 公司也把商业智能套件作为其数据库的一个重点来发展，微软也认为商业智能将是其下一代数据库产品的主要利润点。

7.1.2　数据库的安全特性

数据库系统的安全机制主要有：存取管理、安全管理和数据库加密。存取管理是一套防止未授权用户访问数据库的方法、机制，目的在于控制数据的存取，并防止非授权用户对数据库的访问。安全管理指采取何种安全机制实现数据库操作管理权限分配，通常分为集中控制、分散控制两种方式。数据库加密主要包括：库内加密(以一条记录或记录的字段值为操作单位进行加密)、库外加密(以包含数据库结构和内容的整个数据库为操作单位进行加密)、硬件加密。

1. 存取管理技术

存取管理技术包括用户身份认证技术和存取控制技术两方面。用户身份认证技术包括用

户身份验证和用户身份识别技术。存取控制包括数据的浏览控制和修改控制。浏览控制是为了保护数据的保密性，而修改控制是为了保护数据的正确性和提高数据的可信性。在数据资源共享的环境中，存取控制就显得非常重要。

电子商务和网上银行的迅速发展，使人们认识到数据库中数据的价值，同时也意识到数据库系统可能是脆弱的，用户需要特别的认证。通过用户身份验证，可以阻止非授权用户的访问，通过用户身份识别，可以防止用户的越权访问。

存取控制限制了访问者和程序可以进行的操作，通过存取控制可以防止安全漏洞隐患。DBMS 中对数据库的存取控制是建立在操作系统和网络安全机制基础之上的。一般来说，就存取控制而言，低安全等级的操作系统和网络之上很难建立高安全等级的数据库系统，而高安全等级的操作系统和网络之上建立的数据库安全等级也不一定就高。存取控制的模型有自主访问控制(Discretionary Access Control，DAC)、强制访问控制(Mandatory Access Control，MAC)和基于角色的访问控制(Role-Based Access Control，RBAC)。

2. 安全管理

安全管理指采取何种安全管理机制实现数据库管理权限分配。安全管理分集中控制和分散控制两种方式。集中控制由单个授权者来控制系统的整个安全维护，分散控制则采用不同的管理程序控制数据库的不同部分来实现系统的安全维护。集中控制的安全管理可以更有效、更方便实现安全管理。安全管理机制可采用数据库管理员、数据库安全员、数据库审计员各负其责、相互制约的方式，通过自主存取控制、强制存取控制实现数据库的安全管理。数据管理员必须专门负责每个特定数据的存取，DBMS 必须强制执行这条原则，应避免多人或多个程序建立新用户，确保每个用户或程序有唯一的注册账户来使用数据库。安全管理员能从单一地点部署强大的控制、符合特定标准的评估，以及大量的用户账号、口令安全管理任务。数据库审计员根据日志审计跟踪用户的行为和导致数据的变化，监视数据访问和用户行为是最基本的管理手段，这样如果数据库服务出现问题，可以进行审计追查。

3. 数据库加密

对于一些重要部门或敏感领域的应用，仅有存取管理、安全管理是难以充分保证数据的安全性的，有必要对数据库中存储的重要数据进行加密处理，以强化数据存储的安全保护。数据加密是防止数据库中数据泄露的有效手段。与传统的通信或网络加密技术相比，由于数据保存的时间要长得多，对加密强度的要求也更高。此外，由于数据库中数据是多用户共享，对加密和解密的时间要求也更高，以尽量避免对系统性能的影响。

7.2　数据库安全威胁

数据库是商业和公共安全领域最具有战略性价值的资产，通常都保存着重要的商业机密乃至国家机密，这些信息需要被保护起来，以防止竞争者和其他非法用户获取。很多企业花费很多人力、物力保护敏感信息免受外部攻击者攻击，但来自授权用户的攻击却很容易被忽视。

根据最新的数据库安全报告显示，主要有五个因素可能引发数据库安全问题：安全教育、密码管理、共享账号、权限滥用及审计缺陷。

1. 缺乏安全教育

CompTIA(Computing Technology Industry Association，美国计算机行业协会)于 2009 年对一千多家企业在不同安全强化方式所花费的时间进行调查，结果显示，用户培训被排在第九位(共十位)，仅次于日志文件分析。CompTIA 第 2009 年度信息安全趋势报告表明，接受调查的企业中有 85%表示，对非 IT 人员进行安全培训明显改善了数据泄漏问题。针对数据库系统进行的安全培训，目的必须是确保数据库管理人员能够弄清楚他们处理的数据的重要性和价值，这样他们对待工作就会更加谨慎，才能使用专业的方法保障数据库系统安全。

2. 密码管理问题

混乱的密码管理是另一个常见问题。有的 IT 部门允许数据库管理员设置简单好记的密码，有的强制要求设定复杂的密码，但管理员却把密码写下来贴在显示器上。不管是简单的“弱口令”，还是将密码写下来放到公共场所的方式，都使得数据库系统接近于直接暴露在公共网络中，数据库系统的数据也毫无保密性可言。

3. 账号共享问题

用户之间相互共享账号同样会带来安全问题。有些用户会借用他们同事的登录凭证，还有些人会通过特殊的应用程序来间接登录数据库服务器，以获取数据访问权限，甚至有可能在没有留下任何线索的情况下访问数据库。

4. 权限滥用问题

对数据库系统访问权限的滥用表现在两个方面：一是数据库管理员权限滥用。缺少针对数据库管理员监控机制，数据库管理员拥有数据库系统管理、账号管理、权限分配等数据库系统最高权限。如果数据库管理员利用工作之便，窃取、篡改、毁坏重要业务数据，对数据库安全的影响就非常大。国内某著名网络游戏厂商高管王某非法修改游戏服务器数据谋利就是一个很典型的例子。王某利用职务便利，非法修改网游数据库服务器的游戏装备数据，然后通过网站私下交易出售给其他玩家，非法获利 200 余万，给单位造成难以挽回的重大经济损失。二是合法用户权限滥用。数据库系统的操作管理采用分权管理形式，包括多个账号，如普通账号、用于数据库日常维护的临时账号；如果上述账号权限被内部人员或合作方人员用来窃取、恶意损毁数据库的重要业务数据，在短时间内管理者极难察觉数据被篡改或删除，事后也难以追查取证，造成难以弥补的损失。

5. 审计缺陷

数据库自身日志审计的缺陷主要表现是难以实时监测发现问题。数据库系统自身的日志审计功能可以记录各种数据库系统修改、权限使用等日志信息，但不能帮助管理者及时发现、定位问题。同时，由于不能实时监测报警，因此在数据库异常安全事件发生时，无法第一时间报告给管理者，导致管理者不能及时采取有效措施。此外，面对成千上万条日志记录，很

少有数据库管理员为了寻找几条有用的项目，去查看海量的审计日志条目，如何筛选出有用信息是当前数据库系统普遍存在的问题。

7.3　数据库中的数据保护

7.3.1　数据库中的访问控制

数据库的访问控制(Access Control)是通过某种途径允许或限制用户访问能力及范围的一种方法。访问控制的目的是使用户只能进行经过授权的相关数据库操作。

访问控制系统一般包括主体、客体和安全访问政策。主体(Subject)发出访问操作、存取要求的主动方，通常指用户或用户的某个进程。客体(Object)指被调用的程序或欲存取的数据。安全访问政策指用以确定一个主体是否对客体拥有访问能力的一套规则。

数据库访问控制方式分为：自主访问控制、强制访问控制和基于角色的访问控制三种方式。

1. 自主访问控制(Discretionary Access Control，DAC)

DAC 是基于用户身份或所属工作组来进行访问控制的一种手段。具有某种访问特权的用户可以把该种访问许可传递给其他用户。DAC 允许使用者在没有系统管理员参与的情况下对他们所控制的对象进行权限修改，这就造成信息在移动过程中其访问权限关系会被改变。例如，用户 A 可将其对目标 O 的访问权限传递给用户 B，从而使原来对 O 没有访问权限的 B 可以访问 O。

2. 强制访问控制(Mandatory Access Control，MAC)

MAC 对于不同类型的信息采取不同层次的安全策略。MAC 基于被访问对象的信任度进行权限控制，不同的信任度对应不同的访问权限。MAC 给每个访问主体和客体分级，指定其信任度。MAC 通过比较主体和客体的信任度来决定一个主体能否访问某个客体，具体遵循以下两条规则：其一，仅当主体的信任度大于或等于客体的信任度时，主体才能对客体进行读操作，即所谓的“向下读取规则”；其二，仅当主体的信任度小于或等于客体的信任度时，主体才能对客体进行写操作，即所谓的“向上写入规则”。

3. 基于角色的访问控制(Role-Based Access Control，RBAC)

在 RBAC 中，引入了角色(Role)这一重要概念。所谓角色，就是一个或一群用户在组织内可执行操作的集合。角色可以根据组织中不同的工作任务创建，然后根据用户的职责分配角色，用户可以轻松地进行角色转换。RBAC 根据用户在组织内所处的角色进行访问授权与控制。只有系统管理员有权定义和分配角色。用户与客体无直接联系，只有通过角色才享有该角色所对应的权限，从而访问相应的客体。RBAC 的主要优点在于授权管理的便利性，一旦一个 RBAC 系统建立起来后，主要的管理工作即为分配或取消用户的角色。RBAC 的另一优点在于系统管理员在比较抽象的层次上控制访问权限，与企业通常的业务管理类似。

Oracle、SQL Server 等流行数据库系统均采用基于角色的访问控制方法。例如，Oracle提供了三种标准角色：CONNECT、RESOURCE、DBA。CONNECT 是 Oracle 的简单权限，它只有在对其他表有访问权时才有意义。拥有 CONNECT 角色的用户可建立表、视图、序号、同义词、数据库链接等。拥有 RESOURCE 角色的用户可建立表、视图、存储过程、触发器、函数、索引等。拥有 DBA 角色的用户拥有系统所有的权限。

在实际应用中，通常采用下列访问控制方案。

- 根据应用系统特点，建立几个核心用户，将表、视图、存储过程、触发器、序号生成器等数据库对象建立在相应的核心用户中。
- 根据系统用户的特点，建立各种类型的角色，并将核心用户中的数据库对象的相应权限及一些系统权限授予相应角色。
- 建立一个通用用户默认角色，该角色只有 CONNECT 权限，将该角色授予任一角色，并设置成默认角色。在与数据库连接后，设置使得只有该角色和其他应用需要的角色有效，屏蔽其他角色，以防止权限过大的角色出现而影响数据库系统安全。

7.3.2　数据库加密

数据库的加密通常分为库外加密、库内加密、硬件加密三种方式。

1. 库外加密

因文件型数据库系统是基于文件系统的，故库外加密就针对文件 I/O 操作或操作系统而言。数据库管理系统与操作系统的接口方式有三种：一是直接利用文件系统的功能；二是利用操作系统的 I/O 模块；三是直接调用存储管理。所以在采用库外加密的方法时，可以将数据先在内存中使用 DES、RSA、AES 等方法进行加密，然后文件系统把每次加密后的内存数据写入到数据库文件中去(注意是把整个数据库当作普通的文件看待，而不是按数据关系写入)，读入时再逆方面进行解密就可以正常使用了。这种加密方法相对简单，只要妥善管理密钥就可以了。主要缺点是对数据库的读写都比较麻烦，每次都要进行加解密的工作，会影响读写数据库的操作速度。

2. 库内加密

从关系数据库的对象组成出发，可考虑库内加密的思想。关系型数据库的关键术语有：表、记录、字段，可以针对这几方面形成对应的加密方法。通常，我们访问数据库时都是以二维表方式进行的，二维表的每一行就是数据库的一条记录，二维表的每一列就是数据库的一个字段。如果以记录为单位进行加密，那么每读写一条记录只需进行一次加解密的操作。但是由于每一个记录都必须有一个密钥与之匹配，因此产生和管理各条记录的密钥会比较复杂。以字段为单位的加密与以记录为单位的加密情况相似。

3. 硬件加密

相对于软件加密，硬件加密是指在物理存储器与数据库系统之间加上一层硬件作为中间层，加密和解密的工作都由添加的硬件完成。不过由于添加的硬件与原计算机硬件之间可能

存在兼容问题，此外，在控制数据库读写的时候存在着繁琐的机制，所以这种数据库加密方式应用不太广泛。

7.3.3　数据库的完整性保护

数据库的完整性是指数据库中数据的正确性和相容性。例如，某包含学生信息的数据库中：学生的学号必须唯一，不能与其他人重复；性别只能是男或女；本科学生年龄的取值范围为 14~30 的整数；学生所在的系必须是学校已开设的系。

需要注意区分的是，数据库的完整性和安全性是数据库安全保护的两个不同方面。数据库的安全性用于保护数据库，防止恶意的破坏和非法的存取；数据库的完整性用于保护数据库，以防止合法用户无意中造成的破坏，即防止数据库中存在不符合语义的数据，或者说防止数据库中存在不正确的数据。换言之，安全性确保用户只能做被允许的事情，完整性确保用户所做的事情是正确的，从数据库的安全保护角度来讲，完整性和安全性是密切相关的。

为维护数据库的完整性，数据库管理系统必须具备以下几个功能：①提供定义完整性约束条件的机制；②提供完整性检查的方法；③提供违约处理手段。

1. 数据完整性约束的分类

1) 域完整性

对表字段取值进行约束，规定一个给定域的有效入口，包括数据类型、取值范围、格式、精度等的规定。实现域完整性可以通过 Check 约束、Foreign 约束、Default 约束、Not Null 约束等来实施。

2) 实体完整性

以表记录为单位进行约束，规定一个表中的每一行必须是唯一的。数据库设计者需要指定一个表中的一列或一组列作为它的主键，表中的每行必须含有一个唯一的主键。主键不能为空值，且不能与表中已有行的主键值相同。可以通过列的 Identity 属性、主键约束、唯一性约束等来实现。

3) 参照完整性

在关系数据库中，实体与实体之间的关联同样采用关系模式来描述，通过引用对应实体的关系模式的主键，来表示对应实体之间的关联。参照完整性约束又称为引用完整性约束，是指两个表的主键和外键的数据要对应一致。可以通过“外键约束”、“触发器”、“存储过程”等来实施。

4) 用户定义完整性

以上三种数据完整性约束能够实现数据库中大部分数据完整性，但某些约束条件不能用它们来实现。例如，入学时间不能晚于毕业时间。实现诸如此类的数据完整性保护，需要开发者自己通过创建存储过程和触发器、规则等来实现。

2. 实施完整性的应用实例

通过“约束”可实施列级和表级的数据完整性。例如，SQL Server 支持的“约束”有如下几种：非空约束(Not Null 约束)、主键约束(Primary Key 约束)、唯一约束(Unique 约束)、核

查约束(Check 约束)、外键约束(Foreign Key 约束)、默认值约束(Default 约束)。“约束”的定义可在创建表或更改表时进行。

【例 1】 创建表时定义“约束”。

```
CREATE TABLE STUDENT
( 学号   char(6)   PRIMARY KEY,
姓名   char(8)   NOT NULL,
性别   char(2)   CHECK(性别='男'OR 性别='女'),
政治面貌   char(6);
)
```

以上定义的全为列级数据完整性，定义如下：“学号”列为主键；“姓名”列为非空值；“性别”列通过检验 CHECK(性别=‘男’OR 性别=‘女’)，以保证“性别”字段值为‘男’或‘女’。

【例 2】 创建表时定义“约束”。

```
CREATE TABLE SCORE
( 学号   char(6),
课程名   char(20),
成绩   int,
补考成绩   int,
CONSTRAINT   PK_ID   PRIMARY KEY(学号,课程名),
CONSTRAINT   FK_33   FOREIGN KEY(学号)
REFERENCES STUDENT(学号),
CONSTRAINT   FK_35   FOREIGN KEY(课程名)
REFERENCES COURSE(课程名);
)
```

以上三个“约束”全为表级约束。约束 CONSTRAINT PK_ID PRIMARY KEY(学号,课程名)保证“学号 课程名”非空且唯一；约束 CONSTRAINT FK_33 FOREIGN KEY(学号) REFERENCES STUDENT(学号)、CONSTRAINT FK_35 FOREIGN KEY(课程名) REFERENCES COURSE(课程名)保证该表中的“学号”和“课程名”字段值只能取 STUDENT 表中已存在的“学号”值和 COURSE 表中已存在的“课程名”值。

7.4　备份与恢复数据库

7.4.1　数据库备份

数据库系统在运行过程中，难免会遇到诸如人为操作错误、硬盘损坏、电脑病毒、意外断电或是其他灾难，这些都会影响数据库的正常使用和数据的正确性，甚至破坏数据库，导致部分数据或是全部数据的丢失。因此，数据库备份的目的在于建立冗余数据，也就是备份数据库。

通常数据库的故障可分为 4 类。

- 事务内部故障。有些是可以通过事务程序处理的，比如银行转账中的事务一致性问题。但还有一些是不能由事务程序处理的，比如运算过程中的溢出，并发控制中发生死锁等。
- 系统故障。通常称为软故障，指造成系统停止运行的任何事件，比如系统重启，操作系统故障，突然停电等。
- 介质故障。也称为硬故障，比如硬盘损坏，强磁场干扰等。这类故障的发生几率较小，但是破坏最大。
- 人为故障。人为故障是一种人为的故障或破坏方式，比如病毒感染，用户操作失误等。数据库备份技术，应针对不同的故障类型设置相应机制，以保障数据的有效恢复。为避免数据库灾难，必须采取容错措施，使损失降至最低。容错有硬件容错、软件容错两种方式。

硬件容错是采取双系统方案，即同一个数据库系统在两个计算机系统中同时运行，数据操作在两个系统中同步，两个系统有一定的空间距离，这样，只有两个系统同时损坏才会导致数据库损坏。

软件容错是采取备份与恢复方案，即在数据库正常工作时，做出一个数据库结构与数据的完整拷贝，也就是做出数据库的备份，以便数据库遭到破坏时能够恢复数据库。

1. 数据库备份的概念

数据库备份就是通过特定的办法，将数据库系统相关文件复制到转储设备的过程，如图 7-2 所示。其中，转储设备是指用于放置数据库副本的磁带或磁盘等存储设备。选择数据库备份的依据是：丢失数据的代价与确保数据不丢失的代价之比。数据库备份方法有四种：完全数据库备份、增量数据库备份、事务日志备份、数据库文件与文件组备份。

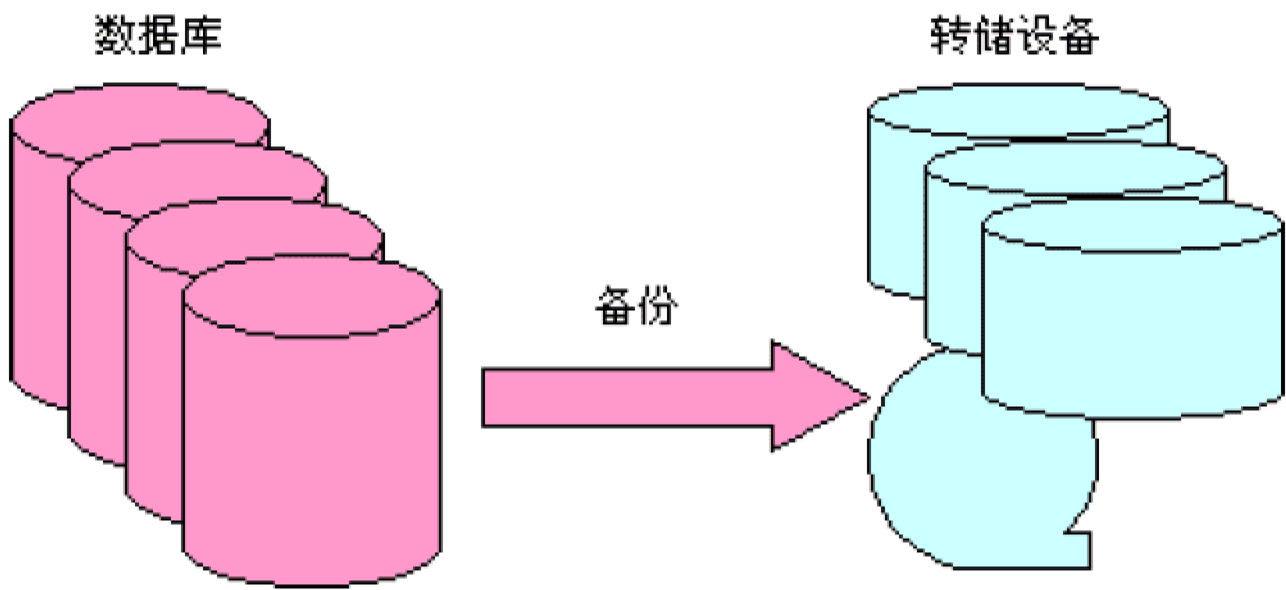


图 7-2　数据库备份示意图

2. 数据库备份的原理

数据库备份的原理在于建立数据冗余。建立冗余数据的方式是进行数据转储和登记日志文件。数据转储在时间上可分为静态转储、动态转储，在空间上可分为海量转储和增量转储。

静态转储就是在转储期间不允许数据库进行任何存取和修改操作。动态转储在转储期间可以进行存取和修改操作，即转储和用户事务可以并发进行。

海量转储是指每次转储全部的数据。增量转储则只转储自上次转储以来更新过的数据。

在事务处理过程中，数据库系统把事务开始、事务结束和对数据库的插入、修改和删除的每一次操作写入日志。一旦发生故障，恢复系统利用日志文件撤销事务对数据库的改变，回滚(Roll Back)到事务的初始状态。或者当数据库文件损坏后，可重新装入备份文件恢复到数据库数据转储结束时刻的正确状态，再利用日志文件把已完成的事务进行重做(Redo)。

3. 数据库备份前的准备

完善的数据库备份操作应当做好充分的准备工作，包括以下内容。

- 确定备份频率。指是每个星期备份，还是每月备份，或者每天备份，甚至在某些情况下，需要每小时备份。
- 确定备份内容。备份数据库需要占用存储空间，会带来成本的增加。因此实际操作中，数据库备份可选择只备份最核心、最关键的数据，以实现投资汇报的合理平衡。
- 确定使用的介质。不同的备份介质，比如磁盘阵列或者磁带机等，在访问性能、访问方便性、读写性能等方面，都有着不同的特性。因此，应根据应用需求、资金状况等情况，选用合适的备份介质。
- 确定备份负责人。数据库备份是一件长期不间断的任务，需要指明具体的负责人专职处理数据库备份工作。
- 确定联机备份或脱机备份。根据应用需求及备份介质的特点，合理选择联机或脱机备份方式。
- 确定是否使用硬件备份。在可靠性要求非常苛刻的应用环境中，仅仅用软件备份还不能满足需求，可能还需要使用硬件备份。
- 确定备份存储地点。条件允许的情况下，应尽可能采用异地备份的方式，将重要的备份数据存放在另外的场所，从而进一步提高备份数据库的可靠性。
- 确定备份存储的期限。备份数据的数据量会随着日积月累迅速增长，在制定备份策略之初，就应权衡备份数据的存储期限。根据应用的具体情况，时间过于久远的、失去价值的数据，应当考虑自动删除，避免占用过多的存储空间。

7.4.2　数据库恢复

数据库恢复就是把数据库由存在故障的状态转变为无故障状态的过程。根据出现故障的原因，数据库恢复分为实例恢复、介质恢复两种类型。实例恢复是当数据库实例出现失效后，数据库系统进行的恢复。介质恢复是当存放数据库的介质出现故障时所做的恢复。

装载(Restore)物理备份与恢复(Recover)物理备份是介质恢复的手段。装载物理备份是将备份拷回到磁盘，恢复物理备份是利用重做日志(即 Redo 日志，物理备份的一部分)修改磁盘上的数据文件(物理备份的另一部分)，从而恢复数据库的过程，如图 7-3 所示。

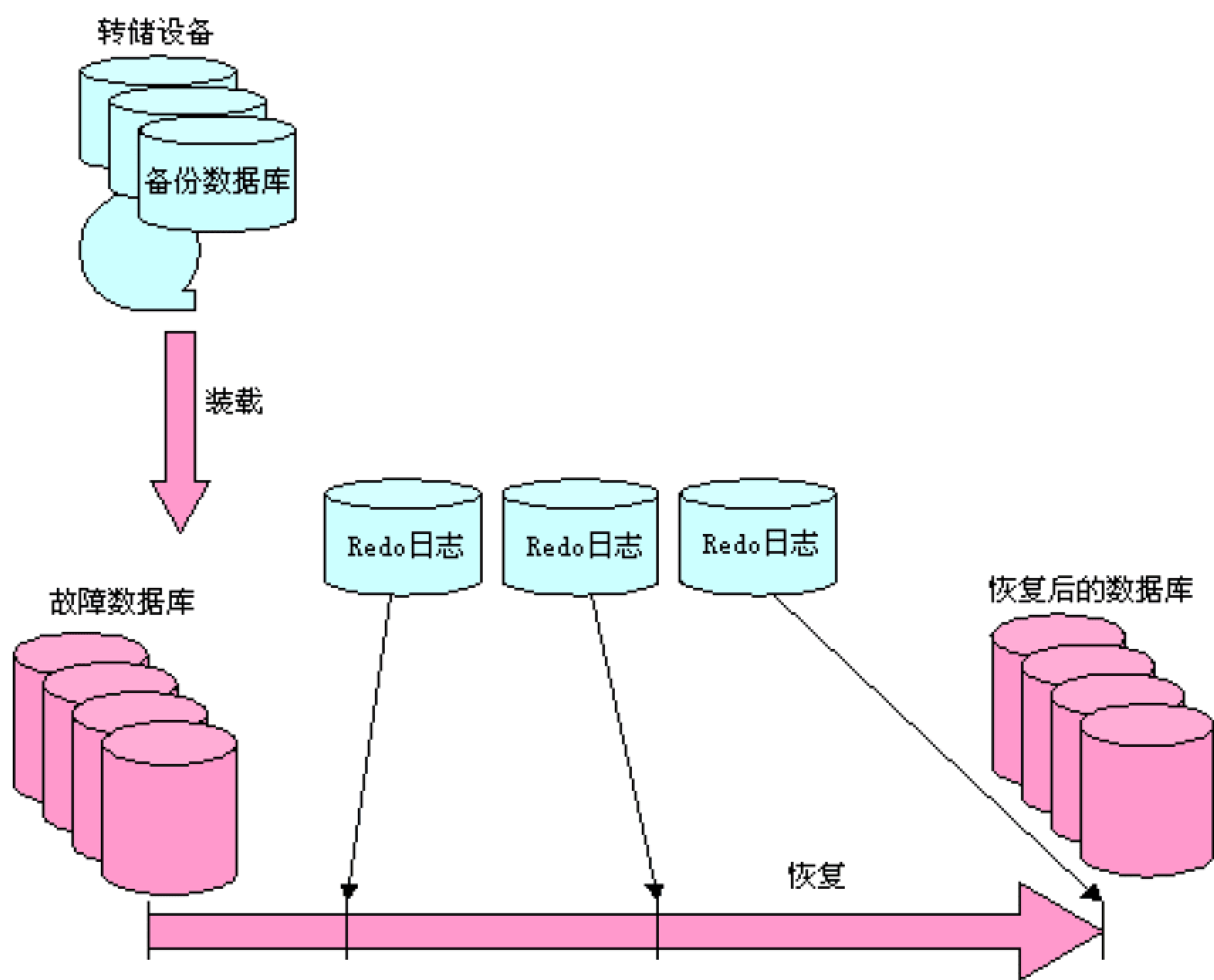


图 7-3　数据库恢复示意图

根据数据库的恢复程度，可将数据库恢复方法分为两种类型：完全恢复、不完全恢复。

- 完全恢复。指将数据库恢复到失效时的状态。这种恢复是通过装载数据库备份，再合并所有的 Redo 日志实现的。
- 不完全恢复。指将数据库恢复到数据库失败前的某一时刻数据库的状态。这种恢复是通过装载数据库备份，再合并部分 Redo 日志实现的。不完全恢复是在完全恢复无法实现，或不需要完全恢复时进行的恢复操作。导致完全恢复无法实现的典型原因是，部分 Redo 日志损坏，使得恢复操作无法继续。

例如，在上午 10 点钟，由于磁盘损坏导致数据库失效，从而中止使用。现在使用两种方法进行数据库的恢复，第一种方法使数据库可以正常使用，且恢复后的数据与损坏时刻(10 点钟)数据库中的数据完全相同，这种恢复方法就属于完全恢复。第二种方法能使数据库正常使用，但只能使恢复后的数据与损坏前 9 点钟时刻数据库中的数据相同，无法恢复数据库到失败时(10 点钟)数据库的状态，这种恢复方法就属于不完全恢复。

7.5　SQL Server 数据库安全机制

7.5.1　SQL Server 安全体系结构

SQL Server 提供了以下四层安全防护。

- 操作系统级别的安全防护。Windows(Windows Server 2003、Windows Server 2008 等)网络管理员负责建立用户组，设置账号并注册，同时决定不同的用户对不同系统资源的访问级别。用户只有拥有了一个有效的 Windows 登录账号才能对网络系统资源进行访问。

- SQL Server 级别的安全防护。SQL Server 通过登录账号设置来实现附加安全层。用户只有登录成功，才能与 SQL Server 建立数据库连接。
- SQL Server 数据库级别的安全防护。SQL Server 的所有数据库都有自己的用户和角色，该数据库只能由它的用户或角色访问，其他用户无权访问其数据。数据库系统可以通过创建和管理不同数据库的用户和角色，来保证数据库不被非法用户访问。
- SQL Server 数据库对象级别的安全防护。SQL Server 可以对所有数据库对象的访问权限进行管理。SQL Server 完全支持 SQL 标准的数据控制语言(Data Control Language，DCL)功能，并通过 DCL 功能保证合法用户即使进入了数据库也不能有超越权限的数据存取操作，即合法用户必须在自己的权限范围内进行数据操作。

从 SQL Server 2005 版本开始，SQL Server 数据库系统增加了许多与安全相关的特性，以帮助保护用户的数据。SQL Server 2005 包含密码策略实施、强大的验证功能和精细的层次权限模型。SQL Server 2005 还含有一个内置数据加密功能，以及内置的加密函数、应用程序编程接口(API)，使用户可以更容易地建立加密安全框架。

密钥管理是加密安全框架中最重要的环节。SQL Server 2005 支持三种加密类型。每种类型使用一种不同的密钥，并且具有多个加密算法和密钥强度。

- 对称加密。SQL Server 2005 支持 RC4、RC2、DES 和 AES 系列加密算法。对称密钥是既可用于加密也可用于解密的单个密钥。使用对称加密可以快速执行加密和解密操作。因此，对称加密非常适合 SQL Server 2005 中大量数据的加密。SQL Server 2005 中，开发人员可以使用一种或多种方法将对称密钥进行加密处理：用户提供的密码、另一个对称密钥、证书的公钥、非对称密钥。
- 非对称加密。非对称密钥由一个私钥及相应的公钥组成。这两个密钥中的每个密钥都可以解密用另一个密钥加密的数据。通常情况下，开发人员使用非对称加密方法加密用于数据库存储的对称密钥。在 SQL Server 2005 中，非对称密钥是公钥和私钥对。公钥不像证书具有特定的格式，因此开发人员不能将其导出至文件。SQL Server 2005 支持 RSA 加密算法以及 512 位、1024 位和 2048 位的密钥强度。
- 证书。使用证书是非对称加密的另一种形式。证书是一个数字签名的安全对象，它将公钥值绑定到持有相应私钥的用户、设备或服务。认证机构 (CA) 颁发和签署证书。用户可以使用证书并通过数字签名将一组公钥和私钥与其拥有者相关联。SQL Server 2005 支持 IETF X.509 v3 规范。用户可以针对 SQL Server 2005 使用外部生成的证书，或者可以使用 SQL Server 2005 生成证书。通常情况下，开发人员使用证书加密数据库中其他类型的密钥。

SQL Server 2005 采用的密钥层次结构框架如图 7-4 所示。与数据加密解密有关的详细内容请参考本书第 5 章“密码学基础”。

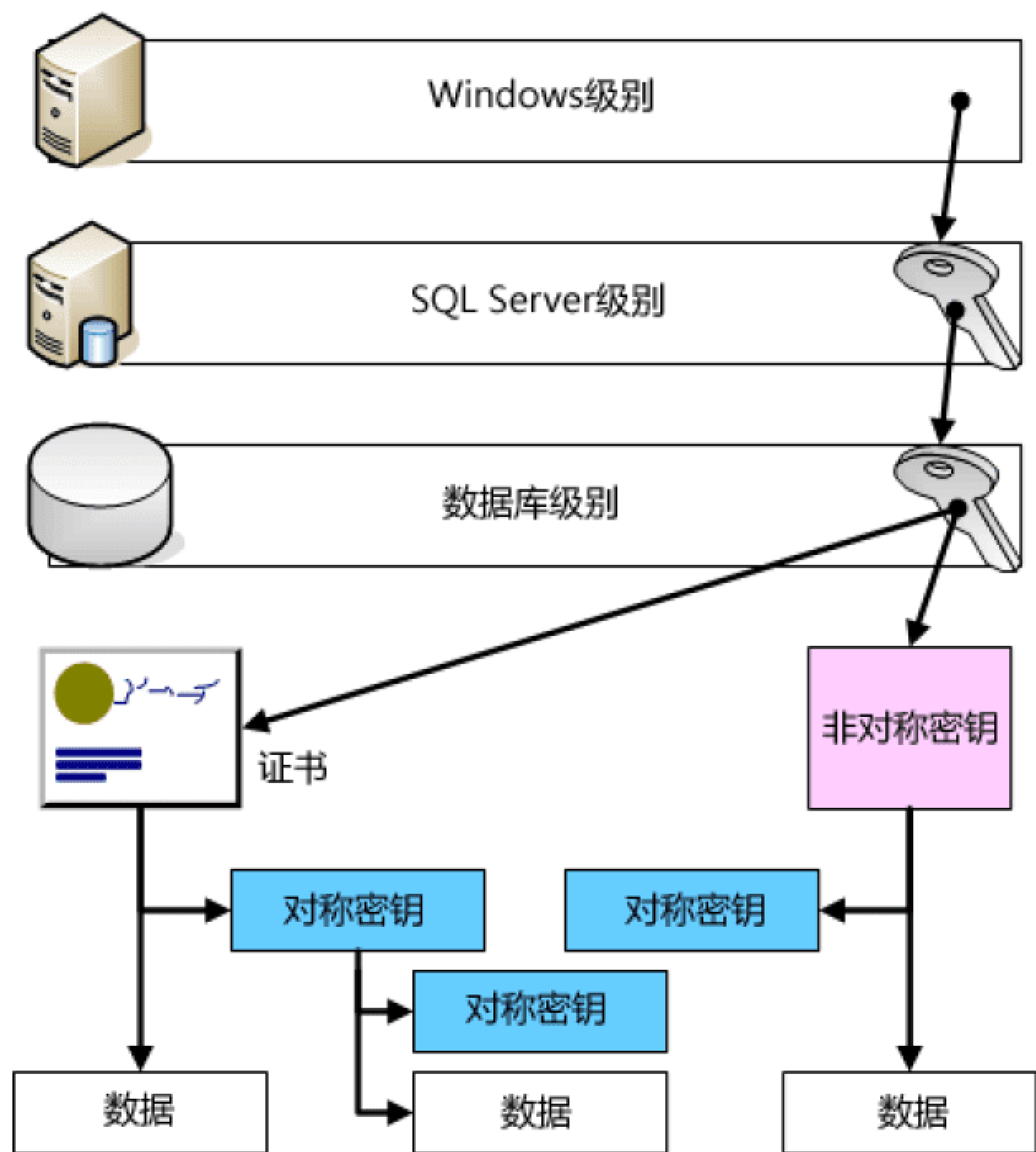


图 7-4　SQL Server 2005 采用的密钥层次结构框架图

7.5.2　SQL Server 身份认证

身份认证是指数据库系统对用户访问数据库时所输入的用户名、口令进行确认的过程。身份认证的内容包括确认用户的账号是否有效、能否访问系统、能访问系统中的哪些数据等。SQL Server 有三种身份认证模式，即 Windows 身份认证模式、SQL Server 身份认证模式、混合模式。

- Windows 身份认证模式。Windows 身份认证模式是指 SQL Server 服务器通过使用 Windows 当前登录用户的权限来控制用户对 SQL Server 服务器的登录及访问权限。它允许一个网络用户登录到一个 SQL Server 服务器后，不必再提供一个单独的登录用户名及口令，从而实现 SQL Server 服务器与 Windows 登录的安全集成。因此，这种模式也称为集成身份认证模式。
- SQL Server 身份认证模式。SQL Server 身份认证模式要求用户必须输入有效的 SQL Server 登录用户名、口令。这个登录账号独立于操作系统的用户账号，从而可以在一定程度上避免操作系统层次上对数据库的非法访问。
- 混合模式。这种模式下，如果用户在登录时提供了 SQL Server 的登录用户名口令，则系统将使用 SQL Server 身份验证对其进行验证。如果没有提供 SQL Server 登录账号或请求进行 Windows 身份验证，则使用 Windows 身份验证对其进行验证。

具体采用哪种身份认证模式，在安装 SQL Server 的时候可根据安装程序界面中的选项，进行相应选择。已经安装的 SQL Server，可使用如下方法设置身份认证模式。

首先，在 SQL Server 企业管理器中，打开 SQL 服务器组，右击需要设置的 SQL 服务器，在弹出的快捷菜单中选择“编辑 SQL Server 注册属性”。然后，在弹出的“已注册的 SQL Server 属性”对话框中，打开“安全性”选项卡，根据图 7-5 所示进行设置即可。



图 7-5　设置 SQL Server 身份认证模式

7.5.3　SQL Server 访问控制

保障数据库安全的主要目标，是通过各种安全机制实现数据库的保密性、完整性和可用性，并确保只有授权用户才能在权限范围内进行操作。访问控制技术是应用最广泛、最有效的安全机制。访问控制策略一般有三种：自主型访问控制(DAC)、强制型访问控制(M　AC)和基于角色的访问控制(RBAC)。DAC 控制能力比较弱，MAC 控制能力过强，且这两种方式都不便于管理。而 RBAC 可有效克服前两种访问控制方式的不足，降低授权管理的复杂性，提高授权的灵活性。SQL Server 的访问控制机制采用的正是 RBAC 方式。

基于角色的访问控制(Role-Based Access Control，RBAC)是近年来在信息安全领域访问控制方面的研究热点和重点。基于角色的访问控制 RBAC 作为一种灵活、直观的访问控制技术在 20 世纪 90 年代迅速发展起来，RBAC 通过引入角色的概念来实施访问控制策略。不同的角色和它所应具有的权限许可互相联系，用户作为某些角色的成员，获得角色所拥有的权限。角色可以根据实际的单位、组织的不同工作职能和权限来划分，依据用户所承担的不同权利和义务来对相应角色进行授权，对于一个存在大量用户和权限管理工作的系统来说，从用户到角色的管理，简化了权限分配的复杂性，提高了安全管理的效率和质量。

美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)颁布的标准RBAC模型由4个部件模型组成，这4个部件模型分别是：基本模型RBAC0(Core RBAC)、角色分级模型 RBAC1(Hierarchal RBAC)、角色限制模型 RBAC2(Constraint RBAC)和统一模型 RBAC3(Combines RBAC)。RBAC0 模型如图 7-6 所示。

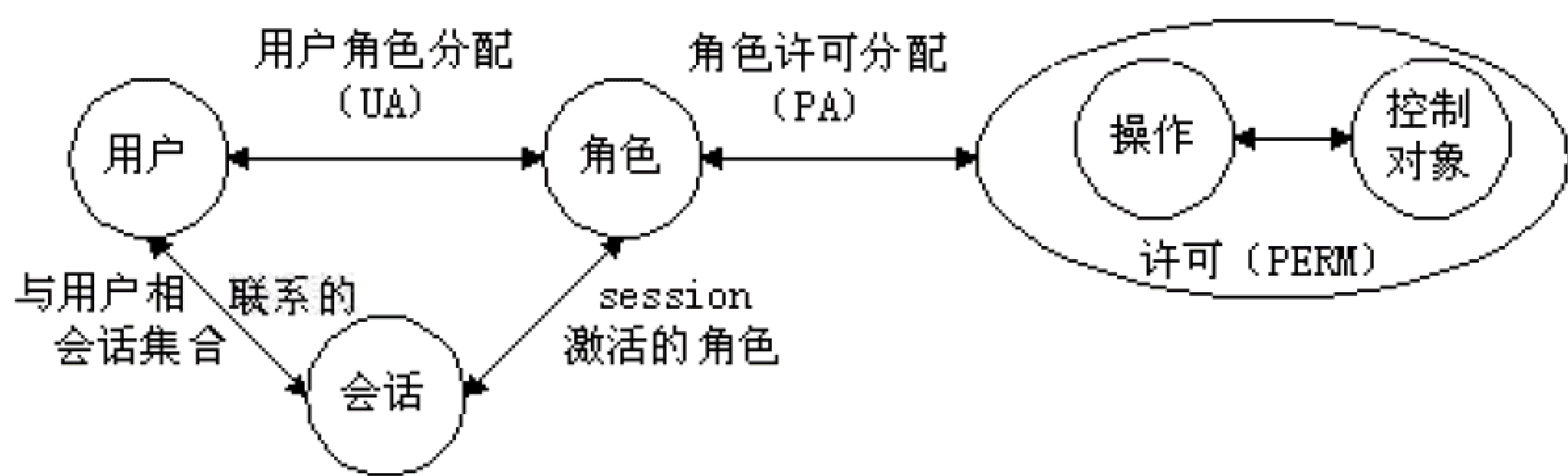


图 7-6　RBAC0 示意图

RBAC0 定义了能构成一个 RBAC 控制系统的最小元素的集合。RBAC 的核心概念包括 5 个基本的静态集合：用户集(Users)、角色集(Roles)、操作集(Operations，OPS)、对象集(Objects，OBS)、权限集(Permissions，PRMS)和一个运行过程中动态维护的会话集(Sessions)。这些集合称为 RBAC 的组件。组件及其之间关系的描述如图 7-6 所示。

在 RBAC 中，权限被赋予角色，而不是用户。当一个角色被指定给一个用户时，此用户就拥有了该角色所包含的权限。会话(Session)是用户与激活的角色集合之间的映射。RBAC0 与传统访问控制的差别在于，通过增加了一层间接性带来了灵活性，RBAC1、RBAC2、RBAC3 都是先后在 RBAC0 上的扩展。角色是一个强大的工具，通过角色可以将用户集中到一个单元中，然后对该单元分配权限。对一个角色授予、拒绝或废除的权限同时适用于该角色的任何成员。可以建立一个角色来代表单位中一类工作人员所执行的工作，然后给这个角色授予适当的权限。当工作人员开始工作时，只需要将他们添加为该角色成员；当他们离开工作时，将他们从该角色中删除。而不必在每个人接受或离开工作时，反复授予、拒绝和废除其权限。权限在用户成为角色成员时自动生效。

如果根据工作职能定义了一系列角色，并给每个角色指派了适合这项工作的权限，则很容易在数据库中管理这些权限。之后，不用管理各个用户的权限，而只须在角色之间移动用户即可。如果工作职能发生改变，则只须更改一次角色的权限，并使更改自动应用于角色的所有成员，操作简洁而灵活。

SQL Server 提供了一些预先定义的用户角色，它们具有一些特定的管理权限。还可为特定环境需求创建定制的角色，然后在数据库上分配权限给这些角色，然后根据人们工作职责的变化从这些角色中添加和删除相应的各个用户。SQL Server 内置的五种角色及其权限、功能如下。

- 结构设计师。定义系统的端对端技术和基础结构设计，并定义项目的前景、范围和互操作性。
- 管理员。运行系统的日常操作。具体而言，包含系统可用性、性能监视和优化、部署、升级、故障排除和配置等各个方面。
- 分析人员。创建供个人使用、也可能供单位中其他人使用的报表和数据模型。分析人员可以是数据处理专业人员，但更多的时候负责分析在完成相关工作过程中获得的企业数据。
- 开发人员。设计、实现并测试网页、报表或应用程序，以实现由结构设计人员设计的整体系统的特定部分。特别是，数据库开发人员设计、实现和测试数据库中的架构和对象(如表和存储过程)。

● 信息工作者。将系统中的可用数据转换为商业信息。

7.5.4 SQL Server 访问审计

数据库安全审计系统是通过对网络数据的采集、分析、识别，实时监控网络中数据库的所有访问操作，发现各种违规数据库操作行为，及时报警，实现数据库安全事件的准确跟踪定位，保障数据库系统安全。根据美国国防部 TCSEC/TDI 标准中关于安全策略的要求，数据库审计是数据库系统达到 C2 级以上安全级别必不可少的一项功能。

数据库安全审计系统首先收集来自用户的事件，当用户进行数据库访问操作时，采集器根据审计数据字典，判断其数据库访问行为是否为审计事件，当数据库访问事件满足审计报警记录条件时，分析器则向管理人员发送报警信息并把用户对数据库的所有操作自动记录下来，存放在审计日志中。

审计日志记录的内容一般包括：用户名、操作时间、操作类型(如修改、查询、删除)，以及操作所涉及相关数据(如表、视图等)等。利用这些信息，可以进一步找出非法存取修改数据库的人员及其修改时间、修改内容等。同时管理人员也可以通过手工查询分析审计信息，并形成数据库审计报告。审计报告通常包括用户名、时间、具体数据库操作(包括采用什么命令访问哪些数据库表、字段)等。

当发现某些数据库访问操作具有潜在危害性，而数据库审计系统的规则库内未制定相应审计规则，则管理人员可以在审计规则库中更新审计规则。在数据库安全审计模型中，数据库审计日志信息起着非常关键的作用，它记录了各种类型的数据库访问事件，为管理人员提供了事后查询的依据，同时可以帮助管理人员实时掌握数据库操作事件的动态信息。

数据库安全审计系统的实现有两种方式：第一种是依靠数据库系统自身具备的审计功能；第二种是使用独立的数据库审计系统。第二种方式的部署结构如图 7-7 所示。通常，采用独立的数据库审计系统效果更好，且对数据库系统的运行效率等影响较小，但独立的数据库审计系统价格都比较昂贵。在经费等条件不允许的情况下，可采用数据库系统自身具备的审计功能来实现数据库审计。

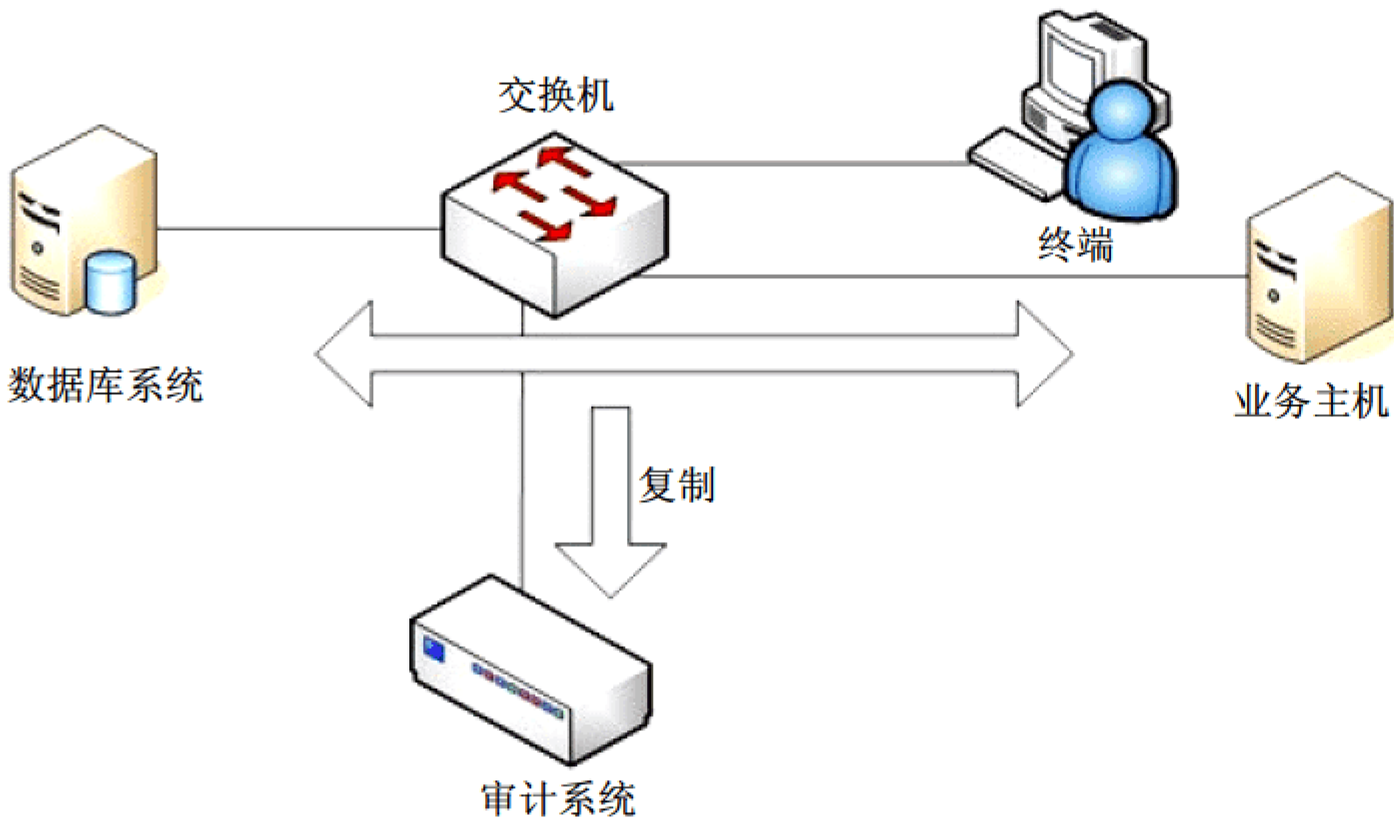


图 7-7　数据库审计系统部署结构

SQL Server 2000 中有一个“事件探查器”工具，它从服务器捕获 SQL Server 2000 事件。事件保存在一个跟踪文件中，可对该文件进行分析，也可在试图诊断某个问题时，用它来重播某一系列的数据库操作。基于这个跟踪文件，可进行数据库系统的审计数据采集，并对这

些审计数据进行分析，判断是否发生入侵如果发生入侵，则把信息保存下来以便系统管理员进行分析。从而实现利用 SQL Server 2000 的跟踪(Trace)技术，全面监视 SQL Server 2000 服务器的性能和活动。它可以帮助管理员了解数据库服务器上的事件和情况。

当事件探查器正在运行时，它能捕获正在向 SQL Server 实际发送的命令。例如，如果某客户向 SQL Server 发送了只由一个存储过程调用组成的批处理命令，就能够捕获和记录每个存储过程中的所有语句，它还能跟踪表的每一次访问、每一次加锁操作、每一次发生的错误，如图 7-8 所示。

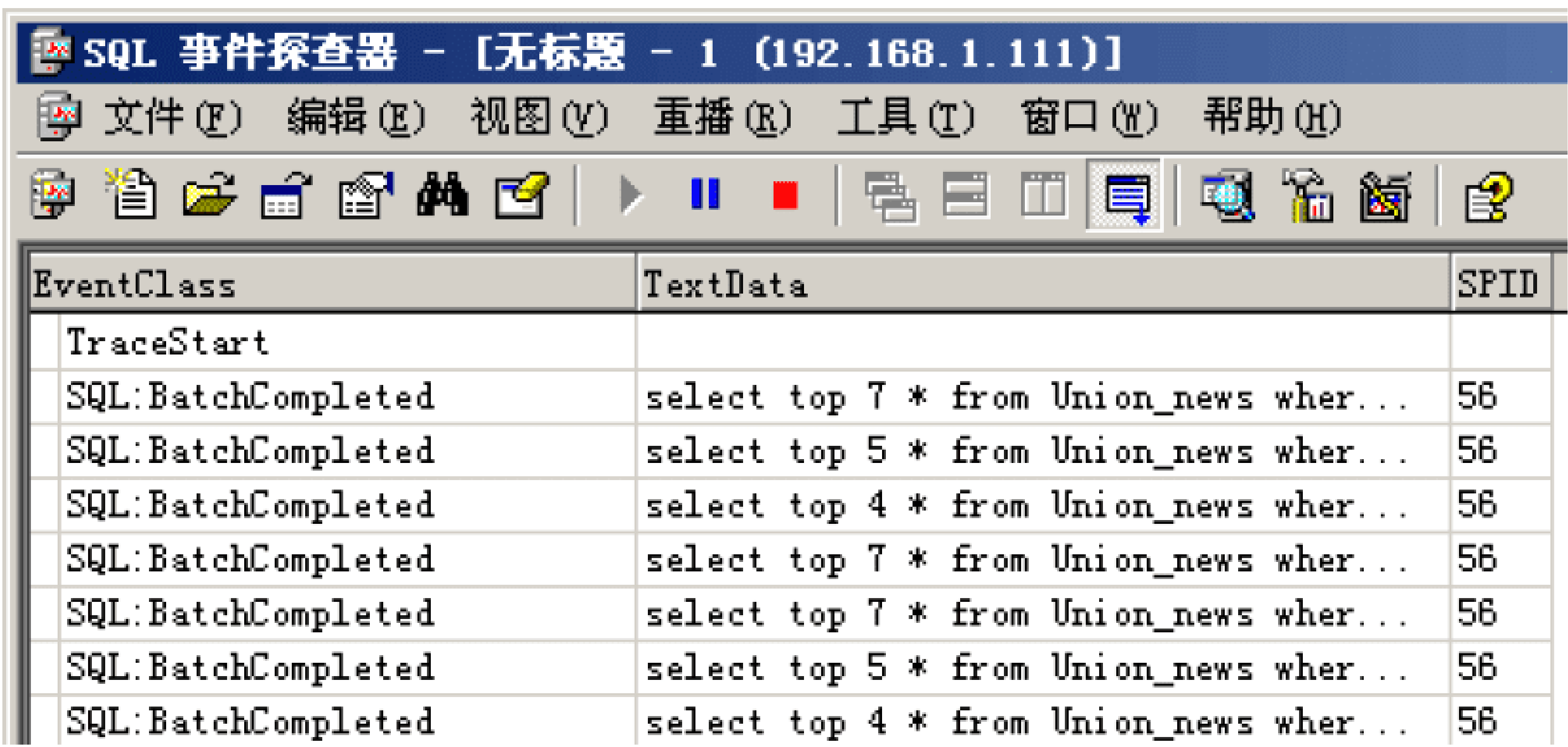


图 7-8　SQL Server 事件探查器

利用 SQL Server 2000 的事件探查器实现的数据库审计功能相对比较弱，SQL Server 2008 的数据库审计功能有了显著增强。在 SQL Server 2008 里实现数据库审计的步骤如下。

(1) 给每个 SQL Server 2008 实例创建一个 SQL Server 审计。

(2) 创建服务器审计规范、数据库审计规范。

(3) 激活 SQL Server 审计。

(4) 查看审计数据。具体操作及相关文档见微软网站 http://msdn.microsoft.com/ en-us/library/cc280526%28SQL.100%29.aspx 的文档。

本 章 小 结

本章介绍了数据库系统的基本概念，数据库系统在迅速发展的信息技术领域的重要作用及面临的威胁。在阐述数据库系统的几种主要保护机制后，介绍了基本的数据库备份、恢复的概念，最后以当前主流关系数据库之一的 SQL Server 为例，介绍典型的数据库系统的安全体系、认证机制、访问控制机制和数据库审计的概念、方法。

课 后 练 习

一、 填空题

1. 数据库系统的安全机制主要有(　　　　　　)、安全管理和数据库加密。

2. 存取控制模型有自主存取控制(DAC)，其缩写来自于英文(　　　　　　)、强制存取控

制(MAC)，其缩写来自于英文(　　　　　　)和基于角色的访问控制(RBAC)，其缩写来自于英文(　　　　　　)。

3. 数据完整性约束分为域完整性、(　　　　　　)、(　　　　　　)、用户定义完整性。

4. SQL Server 的三种身份认证模式，即 Windows 身份认证模式、(　　　　　　)身份认证模式、(　　　　　　)模式。

5. Oracle 采用基于角色的访问控制方法，内置了(　　　　　　)、RESOURCE、DBA 三种标准角色。

二、 选择题

1. 目前市场占有率最高的数据库模型是(　　)。
   A. 层次模型　　B. 关系模型　　C. 网状模型　　D. 以上都不是

2. Oracle 数据库系统采用的访问控制方式为(　　)。
   A. DAC　　B. MAC　　C. RBAC　　D. 以上都不是

3. 某 SQL 语句“CREATE TABLE SCORE ...”的作用是(　　)。
   A. 创建数据库　　B. 创建表　　C. 添加表记录　　D. 创建表字段

4. 数据库不完全恢复操作，则需要(　　)。
   A. 系统日志　　B. 事件日志　　C. 操作日志　　D. Redo 日志

5. 每次转储全部的数据，称为(　　)。
   A. 海量转储　　B. 增量转储　　C. 同步转储　　D. 异步转储

三、 简答题

1. 简述“关系数据库系统”中“关系”的含义。
2. 数据库系统的安全机制主要有哪三种？简述其基本概念。
3. 数据库自主访问控制、强制访问控制和基于角色的访问控制的各自特征是什么？
4. 数据完整性约束分为哪几种类型？
5. 简述 SQL Server 的三种身份认证模式分别适用的场合。

第8章 恶意软件概念及防范

随着网络的广泛普及和应用，网络环境下多样化的传播途径和复杂的应用环境给恶意软件(Malware)的传播带来巨大便利，从而对网络系统及网络上主机、设备的安全构成巨大威胁。

网络已深入到我们工作、生活的每一个细枝末节。科学计算、办公等各行各业的正常运转离不开网络，休闲、娱乐的方方面面也越来越趋于网络化。计算机的小型化和嵌入式系统的迅猛发展，使得我们可以通过手机、个人数字助理(Personal Digital Assistant，PDA)，乃至MP3、MP4 甚至游戏机等小型设备，也可随时随地连入 Internet。

网络的发展、普及速度超出了人们的预料，在人们受益于网络的同时，网络的负面效应日益显现。在 20 世纪 90 年代，病毒主要依靠软盘、光盘等存储介质在不同用户间使用时来传播。当前的病毒则不同，即使足不出户，所使用的计算机也很容易在不知不觉中就被病毒入侵。

通常所说的病毒，按照严格的定义，应称之为“恶意软件”，首先我们需要明确恶意软件的相关基本概念。

本章重点

- 恶意软件的概念及辨析
- 恶意软件的分类及各类恶意软件的主要特征
- 恶意软件运行的主要症状、检测手段
- 恶意软件的基本防范方法

8.1 恶意软件的概念

恶意软件是非用户期望运行的、怀有恶意目的或完成恶意功能的软件的统称。与恶意软件相近的概念还有恶意代码(Malicious Code)，其含义与恶意软件相近，区别在于所描述的粒度不同。恶意代码用于描述完成特定恶意功能的代码片段，而恶意软件则指完成恶意功能的完整的程序集合。

恶意软件的表现形式较多，主要有 Virus(病毒)、Worm(蠕虫)、Bot(僵尸程序)、Trojan Horse(特洛伊木马)、Exploit(漏洞利用程序)、Backdoor(后门)、Rootkit(隐蔽程序)、Spyware(间谍软件)、Spamware(垃圾信息发送软件)、Adware(垃圾广告软件)。

在对恶意软件的名称引用上经常出现混用、指代不明的情况。例如，许多用户将所有导

致计算机工作不正常(如变慢、系统崩溃等)的恶意软件都统称为病毒，将未经用户许可隐藏在计算机内运行的恶意软件都称为(特洛伊)木马等。然而，不同表现形式的恶意软件的工作原理、运行机制以及对系统的破坏和危害都不相同，我们首先需要对恶意软件进行系统的分类，以明确、规范各类恶意软件的概念，区分其间的差异。这样才能以专业的方式对各类恶意软件进行准确表述，进而分析其工作原理，才可能运用合理的防范措施。

8.2　恶意软件分类

各类恶意软件的最终目的，都是要进入目标系统，完成特定任务。我们将入侵目标系统并达到特定目的的完整过程分解为三个阶段：

- 获取对目标系统的远程控制权。
- 维持对目标系统的远程控制权。
- 通过网络远程控制的方式，在目标系统上完成特定业务逻辑。这里所说的目标系统可以是目标主机系统，也可以是目标网络设备。

根据不同恶意软件所完成的功能在完整的入侵过程中所处的阶段不同，我们将恶意软件分为三种类型。

8.2.1　获取目标系统远程控制权类(第一类)

获取目标系统远程控制权类恶意软件的基本特征，是在未授权的条件下，能够利用各种手段获取对目标系统的远程控制权，即具有完整入侵过程中第一阶段的功能。典型的获取目标系统远程控制权的恶意软件有以下几种。

1. Exploit(漏洞利用程序)

这是第一类恶意软件的基本形式。Exploit 利用操作系统或应用程序中存在的缺陷(Bug，又称漏洞)，可达到以非授权的方式远程控制目标系统或提升本地用户权限的目的。具体过程为：构造特定的输入数据并提交给存在缺陷的操作系统程序或应用程序，使这些有缺陷的程序在所构造的输入数据下，正常的程序流程发生改变，转向事先构造的程序。构造的程序被执行后，则可通过网络使未授权用户远程控制目标系统，或使本地普通用户获得更高的权限。

使用 Exploit 获取目标系统的远程控制权后，完整入侵过程中后续的维持控制权、完成特定业务逻辑的工作均与 Exploit 无关。典型的 Exploit 类恶意软件有 Buffer Overflow Exploit(缓冲区溢出漏洞利用程序)、SQL Injection Exploit(SQL 注入程序)等。当操作系统或应用程序的源代码量达到一定规模后，程序中存在缺陷是不可避免的，所以各种漏洞层出不穷，Exploit 类恶意软件也日益增多。

容易造成误会的一个观点是，Windows 系列操作系统的漏洞比 Unix/Linux 系列的操作系统的漏洞多。事实上，目前没有任何有说服力的数据来验证这个观点。造成这个误解的主要原因在于，对普通计算机用户而言，使用 Windows 类系统的用户数比用 Unix/Linux 系统的要多得多，因而 Windows 系统漏洞受害的用户的绝对数量相应也大得多。

2. Trojan Horse(特洛伊木马)

简称为 Trojan(木马)，这是伪装成合法程序以欺骗用户执行的一类恶意软件。使用 Trojan 入侵目标系统的具体过程为：Trojan 首先通过网络或各种存储介质传播到用户处(此时并未运行)，因其具有伪装、欺骗性，常被经验不足或防范意识较差的用户运行(或打开)，木马程序被运行后，释放出其携带的 Backdoor(后门)以实现对目标主机的远程控制，在必要时还可释放出其携带的 Exploit 以提升用户权限。

从利用木马实施入侵的过程可以看出，与 Exploit 仅包含获取远程控制权的功能不同，除包含用于欺骗用户在目标系统上执行的 Trojan Header(木马头部)之外，Trojan 还包含 Backdoor、Exploit 等 Payload(载荷)，这些 Payload 在 Trojan 执行后被释放出来，以维持对目标系统的远程控制，并完成特定业务逻辑。除通过可执行文件的复制、欺骗执行来传播的木马外，更具欺骗性的 Trojan 类型有邮件木马、网页木马、Office 文档木马等，这几种木马往往在用户毫不知情的情况下就被执行了，危害非常大。

目前最为严重的木马传播方式是网页木马。大多数缺乏基本防范措施的上网用户，出于猎奇等心理，在上网浏览过程中，极容易被一些标题“诱人”的网站链接吸引，比如花边新闻、暴力、色情等内容的链接。这类链接的目的网站大部分都存在网页木马，在用户的操作系统没有足够的防范措施时，木马就直接长驱而入，在用户的计算机中运行，并释放其包含的 Backdoor 或 Exploit 等载荷。

另一种令木马广为传播的方式是 Internet 上的软件下载站点。出于使用方便的目的，用户经常需要在网上下载各类应用软件，而这些软件下载站点鱼龙混杂，相当一部分站点中存放的软件已经被“捆绑”了木马。在安装这样的软件时，木马也会得到执行权限。

此外，通过简单的封装操作，将一些实用工具集成到一个软件包里面的方式，也为一些用心不良的人提供了木马传播的机会。典型的案例是“暴风影音”，这是一个集成了免费视频音频媒体播放器和一些编码解码器的软件包。用户安装软件包后，播放器、集成的编码解码器将被安装并关联常见的各类视频、音频文件。但与此同时，软件包还会释放并执行其包含的载荷。“暴风影音”的载荷通常是 Adware(垃圾广告软件)，运行后悄悄在后台执行，让用户的计算机成为其非法谋利的工具。

3. Worm(蠕虫)

蠕虫是具有自我繁殖能力，无需用户干预便可自动在网络环境中传播的一类恶意软件。Worm 利用目标系统的 Weak Password(弱口令)或目标系统中存在的程序缺陷获得对目标系统的远程控制权，并搜集目标系统内的相关信息，从而将 Worm 自身传染至与目标系统有网络联系的其他系统。比如，蠕虫可先传染到某企业内部网出口的计算机，然后通过这台出口计算机传播至企业内部的网络中。

Worm 自身的存在有两种形式，即可执行文件的形式和内存中进程/线程的形式。当以进程/线程的形式存在时，传播过程中 Worm 在目标系统内不涉及文件操作，故通常不会被杀毒软件查出，具有更强的隐蔽性。与 Trojan 类似，Worm 也包含 Payload 部分，以便在成功入侵目标系统后完成特定的业务逻辑，如 CodeRed Worm，其 Payload 部分的功能就对白宫 Web

服务器进行了拒绝服务(Denial Of Service，DoS)攻击。

4. Bot(僵尸程序)

Bot 与 Worm 的共同点在于有自主“意识”，能自动完成某些动作。若某 Worm 的 Payload 部分包含一个 Backdoor，则称该 Worm 为 Bot。可以这样理解，可远程控制的 Worm 即为 Bot。Bot 比 Worm 更进一步，Worm 虽然具有自主繁殖、传播的能力，但其传播出去之后就不再受控，不能根据 Worm 发布者的意图调整行为方式；而 Bot 在传播出去之后依然可以对其进行控制和调整。由此可见，Bot 的危害性比 Worm 更大，制作精巧的 Bot 甚至可以根据发布者的意图对其 Payload 部分进行升级以适应新的环境或完成新的功能。被 Bot 成功入侵的受控主机即为 Zombie(僵尸主机，又称傀儡主机)，一组 Zombie 则称为 Botnet。当前 Internet 上的主要安全威胁之一的分布式拒绝服务(Distributed Denial of Service，DDoS)攻击就是通过向 Botnet 发出针对特定目标的攻击命令来完成的。

5. Virus(病毒)

病毒是依附于宿主文件，在宿主文件被执行的条件下跟随宿主文件四处传播并完成特定业务功能的一类恶意软件。Virus 的结构与 Worm 相似，除包含用于传播自身的 Virus Header(病毒头部)外，还包含用于完成特定业务逻辑的 Payload 部分。Virus 和 Worm 是容易混淆的两个概念。两者的主要区别在于：一是 Worm 的传播无需宿主文件，可通过网络直接将 Worm 自身传播到目标系统，而病毒传播需要宿主文件，病毒只能寄生在宿主文件中。二是 Worm 的繁殖、传播无需人工干预，由 Worm 自主、自动完成，而病毒的传播需要人工干预。例如，病毒的传播依赖于宿主文件的位置改变，宿主文件到哪里，病毒才可能传播到哪里。而且，若宿主文件未被执行，则寄生其中的病毒不会感染目标系统。

第一类恶意软件特性对比见表 8-1。

表 8-1　第一类恶意软件特性对比

	Exploit	Trojan Horse	Worm	Bot	Virus
获取目标系统控制权的能力	√	√	√	√	√
是否包含 Payload	×	√	√	√	√
感染目标系统的模式	主动	被动	主动	主动	被动

表 8-1 中，感染目标系统的模式，是指这种恶意软件的传播是否需要用户参与，或者说是否需要用户进行操作。主动模式意味着不需要用户操作，只要用户的机器连在网络中，就可能被这类恶意软件入侵。被动模式则表明只有用户做了某些操作或动作，这种恶意软件才有可能进入用户的计算机，如果用户什么都不做，这种恶意软件是无法得到执行权限的。

8.2.2　维持远程控制权类(第二类)

获取对目标系统的远程控制权后，通过在目标系统中运行此类恶意软件，以维持对目标系统的持久远程控制。此类恶意软件用于完整入侵过程的第二阶段。

1. Backdoor(后门)

后门是一类运行在目标系统中，用以在未经授权的条件下，提供对目标系统远程控制服务的恶意软件。需要注意的是，Backdoor 与第一类恶意软件不同，Backdoor 的作用是通过其运行以提供对目标系统未经授权的远程控制的服务，而第一类恶意软件需要利用各种手段来达到此目的，即 Backdoor 是以第一类恶意软件为前提的，Backdoor 必须在目标系统上执行后才能提供远程控制的服务，因此必须先使用第一类恶意软件以获得在目标系统上执行程序的权限。第一类恶意软件是 Backdoor 发挥作用的前提和基础，Backdoor 运行后，后续对目标系统的远程控制均通过 Backdoor 提供的服务来完成。

2. Rootkit(隐蔽程序)

Rootkit 的概念起源于 UNIX/Linux 类操作系统，在这类操作系统中，root 代表管理员的用户名，rootkit 最初是指 UNIX/Linux 系统中一组用于获取并维持 root 权限的工具集。发展至今日，被广为接受的 Rootkit 概念是指用于帮助入侵者在获取目标主机管理员权限后，尽可能长久地维持这种管理员权限的工具。在当前的 Rootkit 概念中，获取管理员权限的过程不由 Rootkit 来完成，即 Rootkit 的使用是基于已经获得了管理员权限的假设。

由 Backdoor 的概念可知，Backdoor 仅提供了一条非授权访问、控制目标系统的“通道”，但并不涉及对这条通道的保护，因而这条通道很容易被目标系统上的管理员或网络安全设备察觉或检测到。Rootkit 的作用是尽可能长久地维持对目标系统的远程控制，故其基本任务就是要隐藏 Backdoor 所提供的通道，尽可能使得目标系统上的管理员或安全设备不能察觉、检测到该通道的存在。当前主流操作系统平台下的 Rootkit 已经比较成熟，内核级的 Rootkit 能做到对操作系统中的进程、线程、网络连接、网络数据、网络通信目的地的深度隐藏，以保护目标系统中运行的恶意软件不被检测到。设想一下，一段程序在用户的计算机中运行，但用户看不到该程序对应的进程甚至是线程，也观测不到该程序与外界进行通信的网络连接，观测不到该程序所产生的网络数据，即使能观测到数据，但无法确定数据的目的地到底是哪里，如果这样的程序在我们的计算机里运行，将会是什么样的后果。事实上，这种在操作系统里，将自己彻底隐蔽起来，完全做到“无影无形”，没有任何手段能检测到其存在的 Rootkit，是完全可以实现的。

在实际应用中，Rootkit 通常直接包含了 Backdoor 的功能。因此，可将 Rootkit 理解为带深度隐蔽功能的 Backdoor。

第二类恶意软件特性对比见表 8-2。

表 8-2　第二类恶意软件特性对比

	Backdoor	Rootkit
提供非授权的远程访问通道	√	√
隐藏自身的能力	×	√
隐藏远程访问通道的能力	×	√
隐藏目标系统中运行的其他恶意软件	×	√

由表 8-2 可知，Rootkit 不仅能实现自身在系统中的隐藏，同时还对非授权的远程访问通道进行隐藏。更进一步，Rootkit 还根据需要，对其“保护”下的其他恶意软件进行隐藏。

8.2.3　完成特定业务逻辑类(第三类)

第三类恶意软件用于完成入侵目标系统后最终所要进行的操作，如窃取情报、破坏系统、发动攻击、中转数据等。第一和第二类恶意软件的作用在于为第三类恶意软件提供一个安全、便捷的运行平台。

1. Spyware(间谍软件)

这是典型的第三类恶意软件，用于从目标系统中收集各种情报、信息，如商业、军事情报，用户信用卡号、个人隐私信息及文档，各种网站或邮箱用户名、口令等信息。收集到这些信息后，Spyware 通过网络将其发送给入侵者。在 Rootkit 的保护下，Spyware 本身以及 Spyware 所产生的网络通信都被隐藏，使得 Spyware 可在目标系统中安全地存活下来，极难被受害用户发现。

Spyware 在目标系统中的运行途径主要有三种：一是将 Spyware 放在 Worm、Bot、Virus、Trojan 的 Payload 中，在 Worm、Bot、Virus、Trojan 执行时被释放出来并执行。二是利用 Exploit 获取对目标系统远程控制权后，将 Spyware 通过网络传输到目标主机并执行。三是在目标系统上安装并运行 Rootkit、Backdoor 后，通过其提供的远程控制服务将 Spyware 传输到目标主机并执行。为了提高运行效能，通常使用第三种方式。

2. Spamware(垃圾信息发送软件)

为了避免被追查，Spam(非期望的垃圾信息，如垃圾邮件)的发送者通常不会直接使用自己的主机发送垃圾信息。为了扩大垃圾信息的发送范围，仅仅用一台主机发送垃圾信息是不够的。Spamware 就是运行在大量被入侵主机中，用于发送垃圾信息的恶意软件，Spamware 在目标系统中的运行途径与 Spyware 类似。

3. Adware(垃圾广告软件)

它运行在被入侵主机中，用于以各种方式显示垃圾广告。Adware 在目标系统中的运行途径也与 Spyware 类似。有时用户在进行正常工作时，屏幕界面会突然跳出一些文字或图形对话框，或者是浮动的广告条等信息，这就是典型的被 Adware 入侵的症状。此时，用户也许能定位到这些广告程序对应的进程，并终止这些进程，但很快这些进程又会被创建出来，垃圾广告重新布满屏幕，这种现象很可能是因为这些 Adware 处在 Rootkit 的保护控制状态下。

4. 其他第三类恶意软件

其种类很多，根据具体应用需求不同而不同，如对目标系统进行攻击、破坏的恶意软件有多种不同的类型，但目前尚无统一规范的命名。

8.3　恶意软件的运行症状

对普通恶意软件而言，当其在操作系统中运行时，会表现出一些症状。日常操作计算机时，留心观察操作系统运行的相关状态，有助于在一定程度上检测普通恶意软件。

某系统被恶意软件入侵后的典型症状见图 8-1。

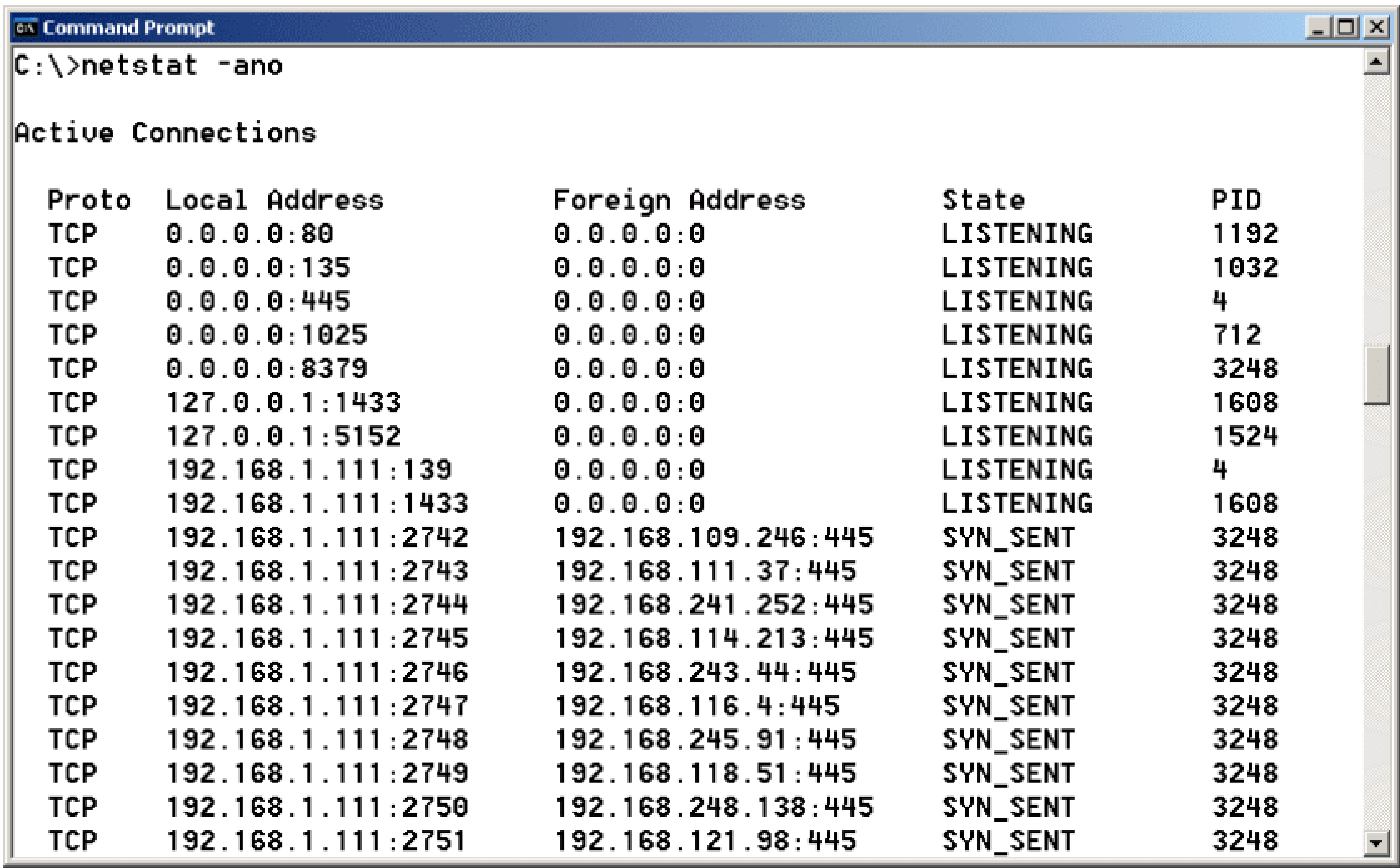


图 8-1　典型恶意软件运行症状

图 8-1 中，使用 Windows 系统内置的网络状态查看命令 netstat，查看当前 IP 地址为 192.168.1.111 的主机当前网络状态。netstat 命令所带参数“o”表示列出执行相关网络操作的进程的进程 ID。由图可见，该主机发出了大量目标地址不定、目标端口为 445 的 TCP 连接请求(对应的 TCP 状态为 SYN_SENT)。TCP 445 端口是 Windows 2000/XP/2003 系统中用于文件/打印共享的端口，默认情况下 Windows 系统的这个端口处于开放状态。但 Windows 系统的多个版本均存在 445 端口漏洞。本例中的恶意软件显然是在随机扫描与主机 192.168.1.1 同处于一个 B 类 IP 地址段的其他主机。由图 8-1 可见，此恶意软件的进程 ID 为 3248。

这个例子来自于一个恶意软件样本。通过不断执行 netstat –ano 命令，进一步观察还可发现，该恶意软件采取的扫描策略并非是持续不断地扫描，而是间歇性的，扫一段 IP，停一会儿，再继续扫。这样做的目的是避免持续不断扫描导致对系统 CPU 占用率的显著提高，从而引起用户怀疑。

系统运行速度变慢是另一种恶意软件导致典型的症状。图 8-1 展示的恶意软件使用间歇运行的方式，不会占用太多 CPU，而另一些不够高明的恶意软件，在运行时会显著提高目标操作系统的 CPU 占用率，从而导致目标主机用户感觉运行速度明显变慢。更严重时，若目标系统同时被多个恶意软件入侵，占用目标系统的大量 CPU 资源及内存资源，此时，目标系统的正常应用将因资源不足而运行缓慢。当前的计算机硬件速度已相当快，用来处理日常办公软件等应用应该很“流畅”，若在使用这类非游戏程序及专业计算处理程序时，感觉计算机反应“迟钝”，则很可能是因为计算机内有非预期的程序在运行，尤以恶意软件存在可能性为大。

若计算机在使用过程中，用户未进行操作，硬盘灯却无故频繁闪动，这也是恶意软件在

运行的症状。当然，系统后台有磁盘碎片整理之类的程序在运行的情况不在此讨论范围。若未运行磁盘优化等后台程序，却出现硬盘频繁读写的情况，则需要引起注意，应查看系统中是否有可疑进程在进行相关操作。

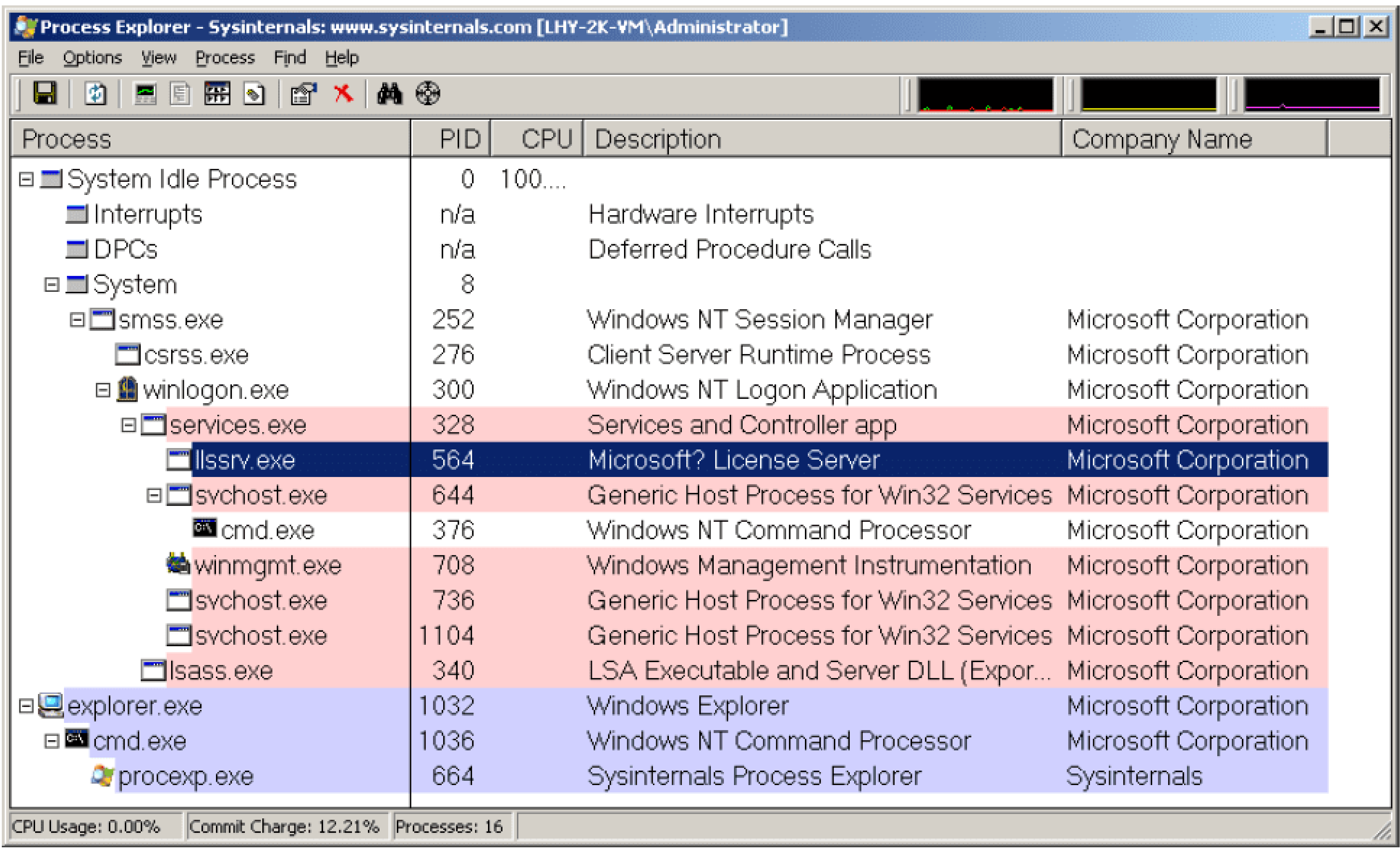


图 8-2　Windows 系统中的常见进程

然而，查找可疑进程并不是一件容易的事情。要了解哪个进程可疑，必须要了解、熟悉正常状态下系统里有哪些进程。图 8-2 里列出了 Windows XP/2003 系列操作系统中常见的进程。图中进程列表是用最专业的进程查看工具——Process Explorer 列出的。这个工具系列前几年已被微软收编，目前工具的最新版本及相关其他工具可以从微软站点 http://technet.microsoft.com/en-us/sysinternals/default.aspx 下载。也可以使用其原始地址 www.sysinternals.com，根据用户操作系统设置的语言类型进入相应语言版本的站点。

由图 8-1 可见，该工具列出了进程的名称、进程 ID(PID)、进程的 CPU 占用率、进程的描述、进程可执行文件的公司信息，其中进程描述和公司信息都来自于进程对应可执行文件内包含的编译信息。双击某进程，则可查看该进程的详细信息，如进程可执行文件的完整路径、进程内包含的线程、进程的网络操作状态等。通过进程的这些详细信息，可以大概判断一个进程的可信程度。需要注意的是进程的描述、公司信息是可执行文件编译时填写的属性，很容易被伪造，只能作为判断的参考。

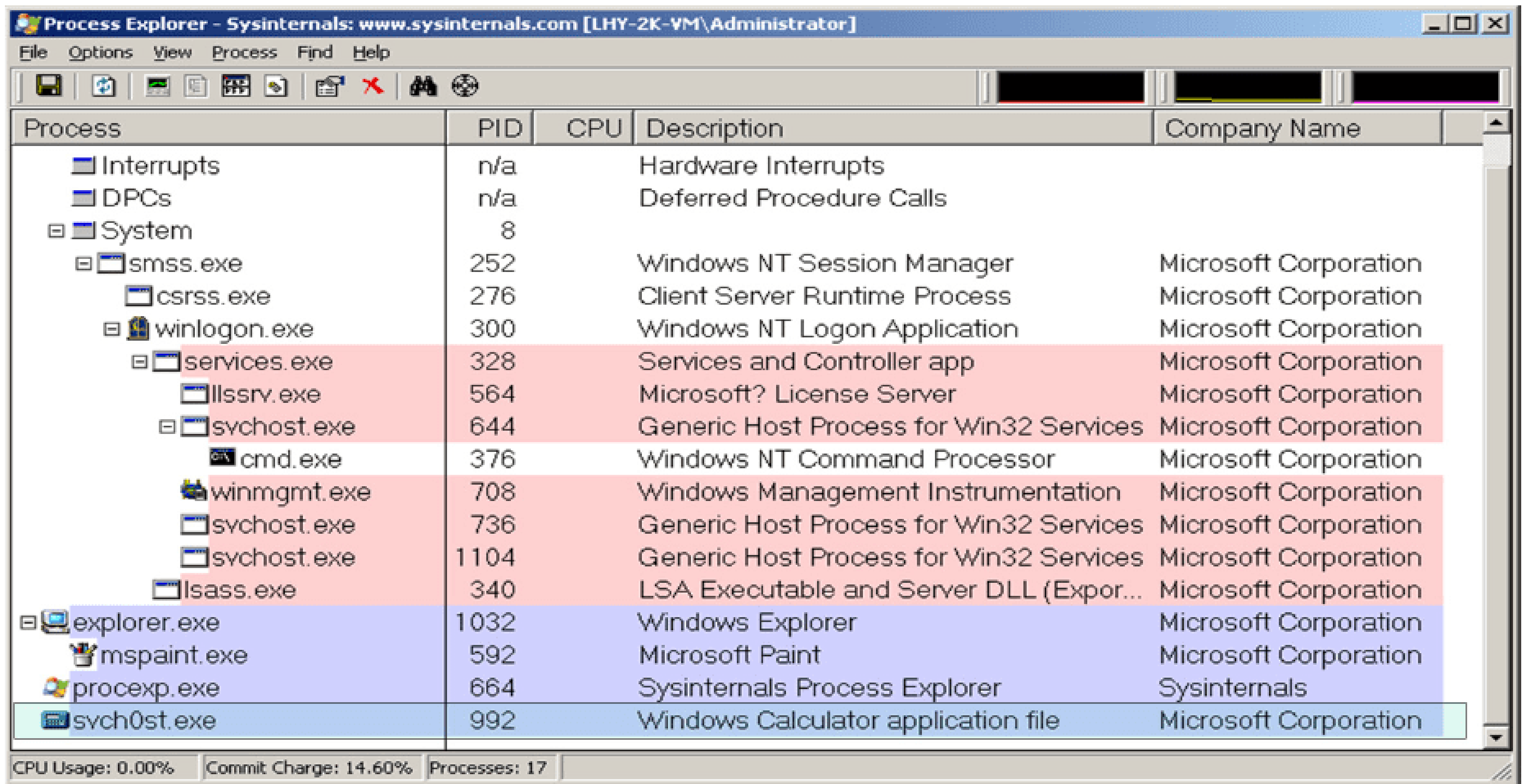


图 8-3　假冒 Windows 系统进程示例

图 8-3 是用于说明恶意软件常用的假冒系统进程的一个例子。图中深色框内的进程“svch0st.exe”(文件名的倒数第三个字符为数字 0)，其可执行文件来自于 Windows 系统自带的计算器程序“calc.exe”，这里伪装成系统进程“svchost”(倒数第三个字符为小写字母 o)，如果再将“calc.exe”的可执行文件图标改成和“svchost.exe”一致，并将文件描述、公司信息都进行相应修改，则很容易欺骗用户，误以为“svch0st.exe”是一个系统进程。

检查系统中是否有非预期的网络通信，是了解系统中是否有恶意软件在运行的基本方法。恶意软件入侵目标主机后，必然会与外界进行通信，这个通信过程或许频繁，或许是间歇性的，仔细观察所用计算机与外界的通信，则能从一些蛛丝马迹中找出恶意软件的动作痕迹。若系统中没有网络相关操作的程序在运行，使用 netstat 命令查看当前网络状态，则应当如图 8-4 所示，除了本地几个 TCP 端口处于监听(Listening)状态、几个 UDP 端口处于开放状态外，系统没有与外界其他任何主机有网络联系。

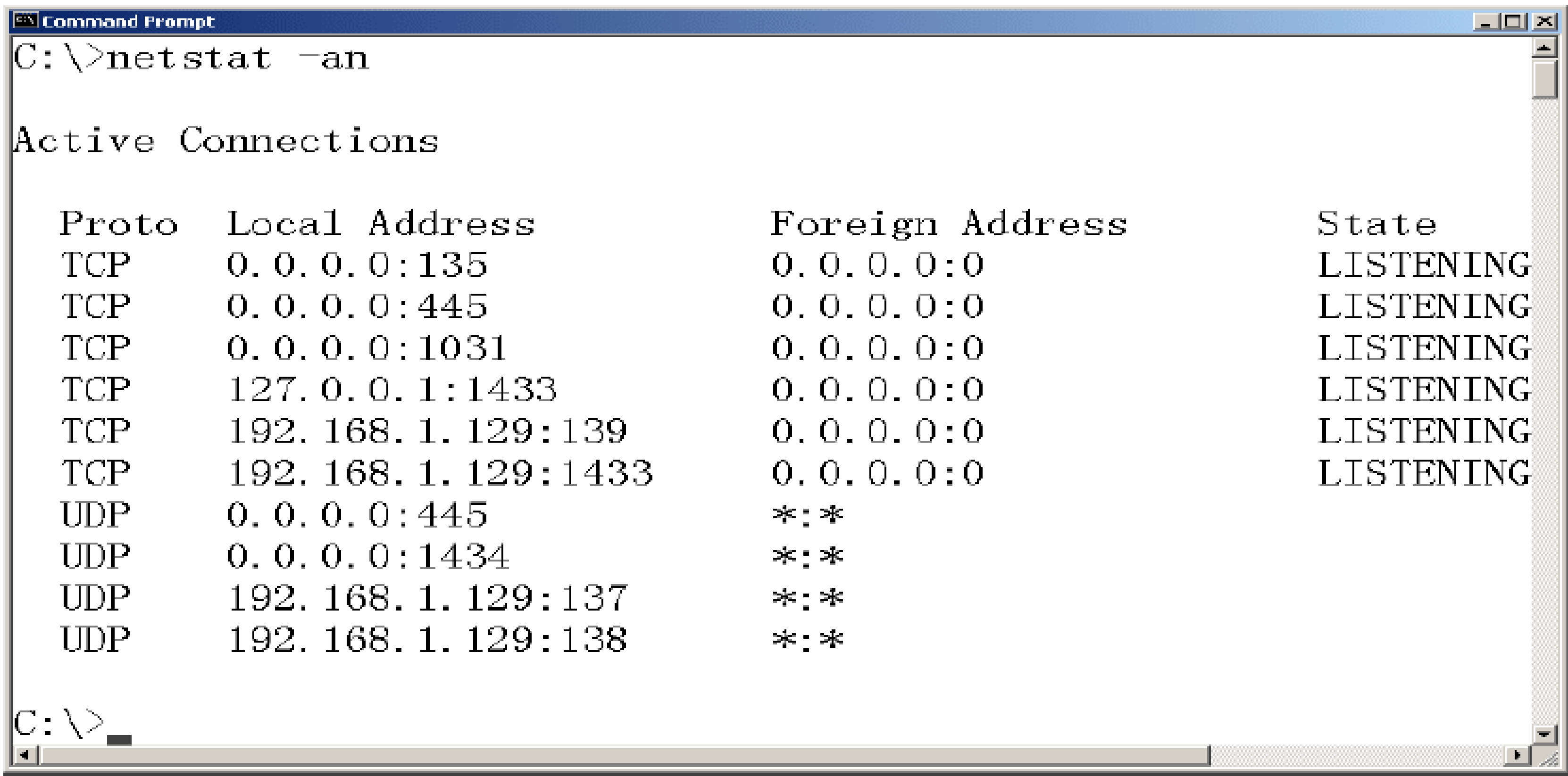


图 8-4　检查非预期的网络通信

图 8-4 所示的情况比较理想，实际系统运行情况会复杂一些。例如，安装的杀毒软件可能会定期和服务器联系，看有无病毒库更新或者操作系统补丁自动升级程序会定期联系微软的网站看有没有新的补丁等。此时，为了准确判断，应当先结束所有可能产生网络通信的进程，然后在 netstat 命令后加上参数“-o”查看进行网络操作的进程 ID，然后使用 tasklist 命令查看相关进程 ID(PID)对应哪个进程，如图 8-5 所示。如果想了解关于该进程的详细信息，可使用图 8-3 所示的工具“Process Explorer”。

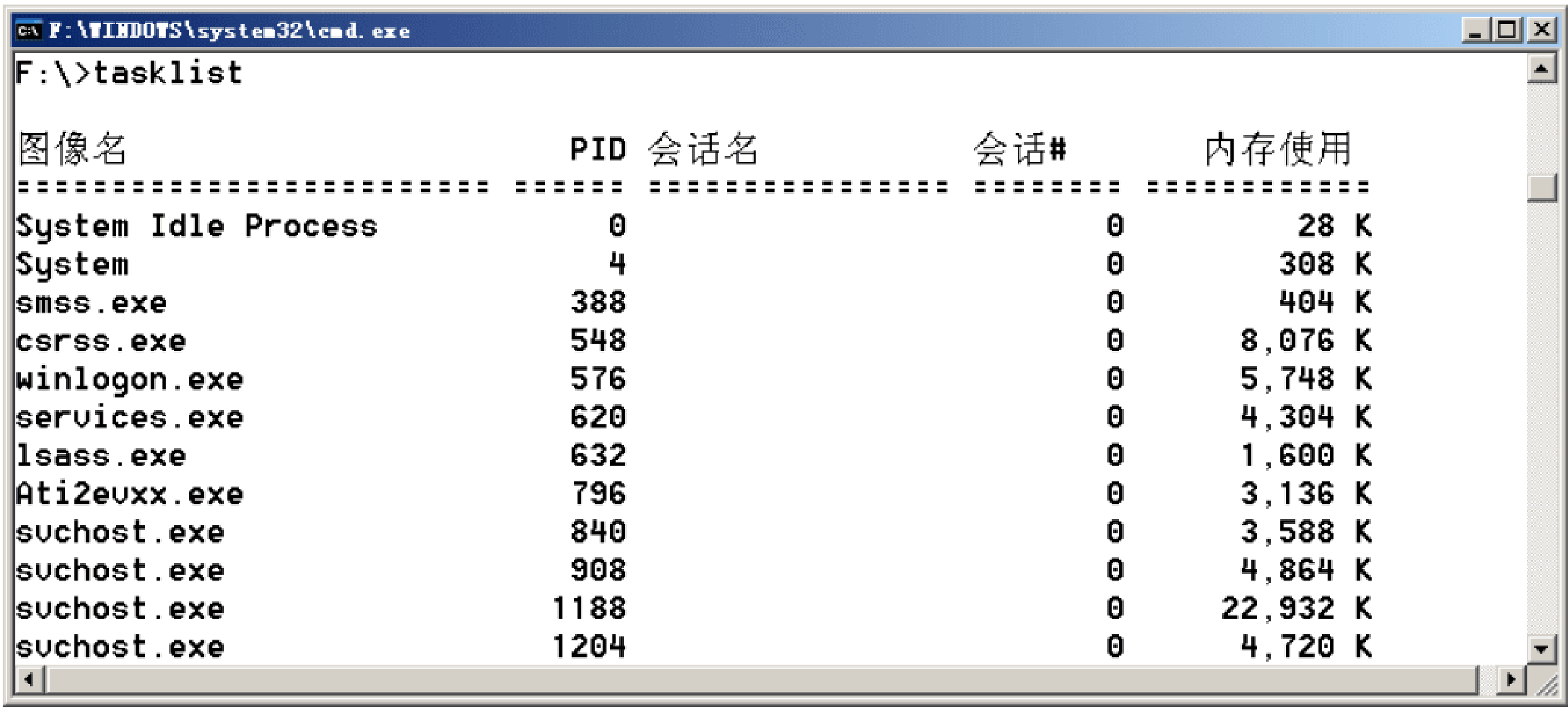


图 8-5　查看 PID 对应的进程

除了前述系统运行速度变化、磁盘读写异常、异常进程出现、非预期的网络通信外，若发现系统中有无缘无故新增加的文件，或者某些文件的文件日期、文件图标等发生非人为的变动，则可能是系统中有了恶意软件。所以在日常使用计算机的过程中，需要多留心系统运行中的一些细微变化，因为许多细微的改变可能就意味着系统运行状况的改变。

恶意软件会用各种办法来隐藏自己，限于恶意软件作者的水平，并非所有恶意软件都能实现 8.2.2 节中所述的 Rootkit 的隐藏效果。但是，即使是使用简单的隐藏手段，也能欺骗相当多的用户。图 8-6 所示是 Windows 系统中的 Folder Options(文件夹选项)对话框，这个对话框的设置决定 Windows 的资源管理器以什么样的方式显示文件列表。这个对话框的打开方式是：在资源管理器中，选择菜单“工具”→“文件夹”选项，在弹出的界面中选择“查看”，即出现图 8-6 所示的界面。

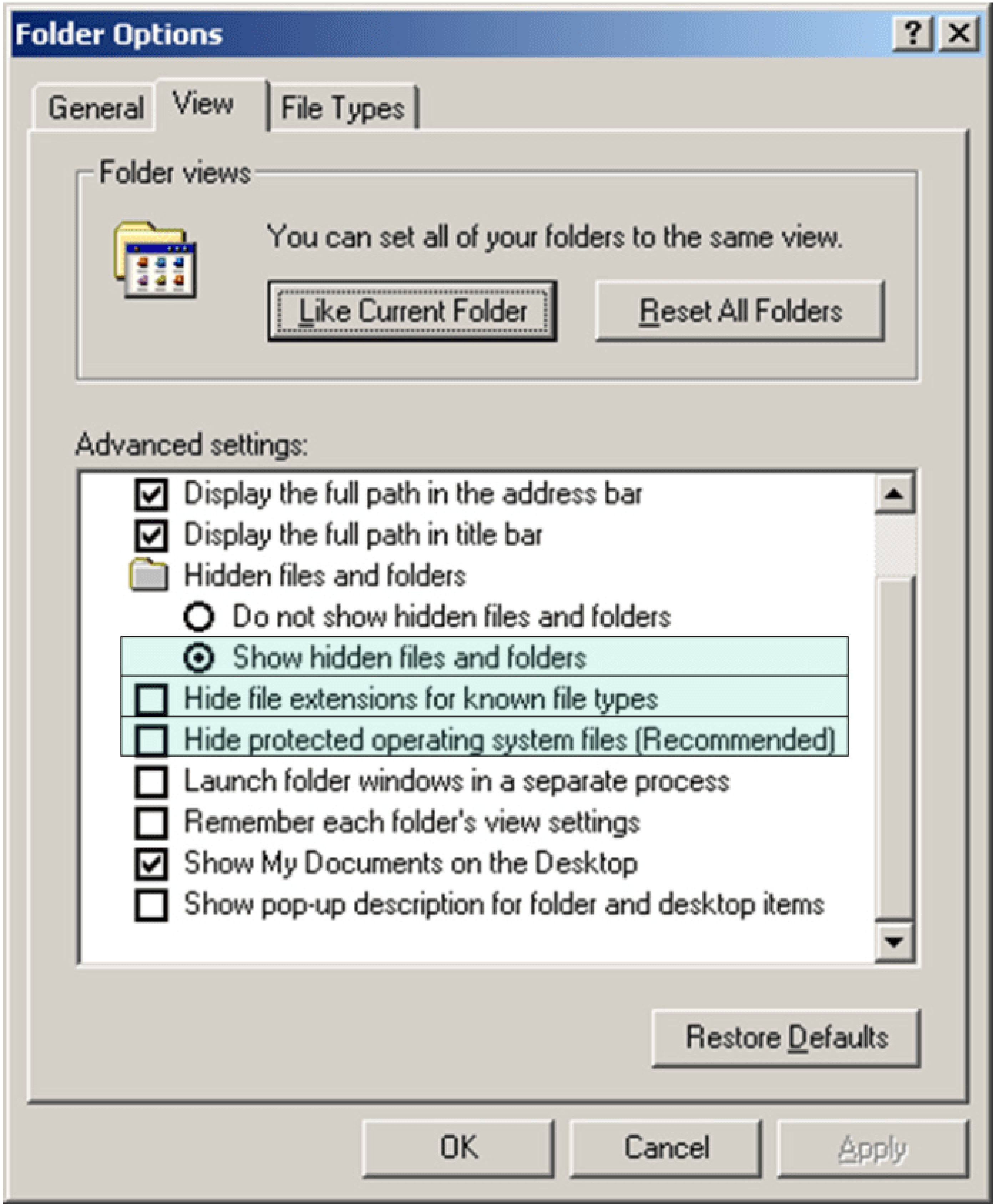


图 8-6　正确设置文件夹选项

图 8-6 所示的是正确的设置方式。我们主要关注深色区域部分的几个选项，这几个选项是 Windows 系统(特别是 Windows XP)的默认设置选项，非常弱智，很容易造成用户被各类简单的恶意软件欺骗。

在图 8-6 中，应选中 Show hidden files and folders(显示隐藏的文件和文件夹)单选按钮，如果不选中该单选按钮，则恶意软件只需简单地修改文件的“隐藏”属性，文件就不会在资源管理器中列出。

在图 8-6 中应取消选中 Hide file extensions for known file types(隐藏已知类型文件的扩展名)复选框，否则 Windows 系统会将大多数文件的扩展名忽略不显示。例如，某个可执行文件的完整文件名为“test.exe”，若选中该复选框 Windows 会认为“.exe”文件是已知类型文件(可执行文件)，则不显示其扩展名，在资源管理器中就只列出“test”。恶意软件可以利用

这个特点，将某个木马可执行文件改名为“test.doc.exe”，则在第二个选项错误的设置下，Windows 资源管理器里列出的是“test.doc”，同时木马的可执行文件图标也被修改为 Word 文件的图标，用户很容易就被欺骗了，误以为这是一个 Word 文档，一旦尝试打开，则木马进入了用户的系统。如果恶意软件的发布者将这个全名为“test.doc.exe”文件改名为“最新内幕消息.doc.exe”之类的文件名，则上当受骗的用户会大大增加。

在图 8-6 中也应取消选中 Hide protected operation system files(隐藏受保护的操作系统文件)复选框，否则恶意软件只需修改系统文件属性，即可伪装成所谓的“操作系统文件”，因而必须让所有的文件都显示出来，不管是不是真的操作系统文件。

8.4　恶意软件的防范

恶意软件的防范，需要根据恶意软件的不同类型，采取不同措施。

针对获取目标系统远程控制权类，首先需要做到的基本要求是及时更新补丁。更新补丁包括更新操作系统补丁和各种应用程序的补丁。操作系统的补丁不更新，很可能让入侵者在网络上无声无息地就进入受害者的系统。应用系统的补丁不更新，则会导致即使在正常操作下也会因为应用软件的漏洞而被入侵，如典型的 Office 系列漏洞。作为正常运行状态，用户打开一个 Word 文档，或者 Excel 文档、PowerPoint 文档，不应当出问题，但是在利用 Office 软件漏洞的前提下，通过精心构造的 Word 等文档，能使得用户在打开文档的同时，恶意软件被执行，从而导致系统被入侵。

在操作系统补丁、应用系统补丁及时更新的基础上，要想不被获取目标系统远程控制权类恶意软件入侵，还需要用户在使用计算机时格外小心，即彻底杜绝打开来历不明的文件。无论是可执行文件，还是 Office 文档、PDF 文档，甚至是 RMVB 等视频文件。所有这些不同类型的文件中，都可能附带恶意软件，在这些文件被执行或打开时，恶意软件即被释放并入侵系统。

但是，辨别来历不明的文件并不容易，特别是非专业用户更容易被欺骗、诱惑。为了将损失降到最低，在操作计算机时，应该遵循信息安全保障的一条基本原则，即“最小权限原则”。也就是说，只给操作计算机的用户分配基本的、最小的、必备的权限。采用最小权限原则的典型案例有银行、超市等场所的终端计算机，这些场所的计算机只需处理相关的基本业务，无需任何其他功能，因而只为这些终端操作用户提供基本的业务处理界面，无需也不进入任何其他界面，这样才能保障终端计算机的正常有效运转。

对普通个人计算机用户而言，最小权限原则应当以这样的方式来实施：当用户安装完操作系统(尽可能使用原版操作系统)、操作系统补丁、日常所需应用软件(尽可能使用官方提供的软件光盘或官方网站下载的版本)、应用软件补丁后，应立即建立一个普通用户账号，然后登出(Logout)管理员账号(Windows 系统的管理员用户名为 Administrator)，再以普通用户账号登录。日常的工作全部都以普通用户账号来操作。在普通用户账号状态下，即使用户计算机被恶意软件入侵，所造成的破坏也比较有限，不会导致计算机被恶意软件彻底控制。除非万不得已，比如需要安装某些涉及系统低层功能(如驱动程序、系统服务程序)的软件，在保障

软件来源可靠的前提下，用户方可登出普通用户，以管理员身份登录进行相关操作，完毕之后立即切换回到普通用户身份。这种操作模式对普通用户而言确实带来一些麻烦，但安全和麻烦是一对如影随形的兄弟，方便就带来安全风险，麻烦相对则能降低风险。

避免被获取目标系统远程控制权类恶意软件入侵，对操作系统的安装也有要求。在恶意软件存在的网络环境中的测试表明，如果在更新操作系统补丁之前就将计算机接入网络，网络中的恶意软件会在很短时间内发现这台未更新补丁的主机，并立即利用系统漏洞感染、入侵该主机。因此，正确的做法是，在安装操作系统之前，就应当将操作系统的最新补丁程序准备好，并将主机从网络中断开，待操作系统安装完毕、补丁更新完毕后，方可将主机接入网络中。

针对维持远程控制权类恶意软件，基本的防范手段是安装杀毒软件及防火墙，对系统内所有的文件操作进行监控，并定期对系统进行扫描，同时阻止来自其他未授权计算机的网络连接。此外需要关注信息安全动态，当出现新的恶意软件时，及时使用专杀工具对系统进行完整扫描。在此基础上，注意经常关闭网络应用程序，以检查系统有无非预期的网络通信动作。

然而，杀毒软件、恶意软件专杀工具等，都只能利用恶意软件的特征码进行扫描，而出于某些特殊目的，网络上的某些恶意软件并没有被各大杀毒软件厂商捕获到样本，因而不可能被任何杀毒软件查出。所以，过于依赖杀毒软件，认为安装了杀毒软件并及时更新病毒库就可以高枕无忧，是很不明智的行为。

对完成特定业务逻辑类恶意软件的防范，与维持远程控制权类恶意软件防范类似，只能通过杀毒软件、专杀工具对系统进行扫描。基于前述理由，这种手段只能起到一定程度上的辅助作用。

综合来看，当前的恶意软件种类繁多、变种更新频率很快，仅靠杀毒软件等方法，都只能对恶意软件的清除起到有限的作用。一旦恶意软件入侵到系统中，往往会对系统造成破坏，因而很难彻底清除。在很多情况下，只能通过格式化系统分区、重新安装操作系统的方式来对系统内的恶意软件进行清除。

但是，即使格式化分区，甚至格式化整个硬盘的所有分区，乃至将硬盘所有分区都删除再重新分区，也不能保证恶意软件就被彻底清除了。因为我们所使用的硬盘的第一个扇区(一个扇区包含 512 个字节)，称为 MBR(Master Boot Record，主引导记录)，在以上格式化、重新分区等动作中，MBR 的开头一段代码以及紧跟 MBR 的后续几十个扇区的数据，都不会受到影响。如果恶意软件存在与这些不受格式化、分区影响的区域，自然不会被清除。

如果我们使用工具软件，例如磁盘编辑工具，将上述 MBR 等扇区的内容清除，是不是就彻底清除了所有的恶意软件呢？结果并不是这样。

回答这个问题，我们需要了解计算机的启动过程。对 x86 架构的计算机而言，在其上电的一瞬间，执行的是 FFFF:0000 地址处的程序代码，而此处的程序代码来自于主板的 BIOS 芯片，上电后的自检过程中会检查显卡、网卡等外设。如果需要，则执行显卡、网卡的 BIOS 里面的相关初始化程序。由以上过程可知，如果恶意软件驻留在主板 BIOS 芯片，或者显卡网卡 BIOS 芯片，乃至网卡的启动芯片里，则无论我们怎样格式化硬盘、清除硬盘 MBR，或者低级格式化硬盘，都丝毫不会影响到恶意软件的存在。更为可怕的是，在这样一台在上电

的同时恶意软件就已被执行的计算机上，是无法用任何手段检测出恶意软件的存在的。因为恶意软件最先获得了控制权，即使使用工具来检测主板 BIOS 等的内容，得到都是虚假信息。事实上，相关资料表明，这类基于主板 BIOS 的 Rootkit 已经有现实中的版本。

由上述分析可知，一旦计算机被恶意软件入侵，特别是在管理员权限下，可以对计算机进行任何操作，包括对计算机的所有硬件(如主板 BIOS 等)的操作。如果遇到上述高级 Rootkit，则通过这台计算机本身是根本无法实现对恶意软件的检测、清除的。

因此，需要从源头控制恶意软件的入侵，也就是尽最大努力做好针对第一类恶意软件 ——维持远程控制权类恶意软件的防范，从源头上堵住恶意软件。以断开网络安装操作系统为前提，在安装好系统补丁、可信来源应用软件、应用补丁，开启防火墙后，以普通用户身份来操作计算机。在这样的普通用户身份环境下，即使运行了恶意软件，由于普通用户权限不能直接操作硬件，也能将恶意软件的入侵概率尽可能降低。

本 章 小 结

本章从一次完整入侵的过程分析，归纳出三种类型的恶意软件，并对三类恶意软件的工作机制、主要功能、特征进行了剖析。在总结各类恶意软件运行症状的基础上，阐述了清除恶意软件的困难之处，总结出有效防范恶意软件的基本原则在于从源头控制、防范，并给出了防范要点。

课 后 练 习

一、 填空题

1. Worm(蠕虫)、Virus(　　　　　)是两类早期出现的恶意软件形式。

2. 根据恶意软件在入侵过程中所处不同阶段，恶意软件通常可分为获取远程控制权类、(　　　　　)类、完成特定业务逻辑类三种类型。

3. 查看当前主机网络连接状态的命令是(　　　　　)。

4. 格式化硬盘并非一定能将恶意软件从硬盘内清除干净，主要是因为恶意软件可用从硬盘的(　　　　　)获得执行权限。

5. 防范恶意软件通过 Office 文档进行传播的主要手段是为 Office 系统(　　　　　)。

二、 选择题

1. 恶意软件中，Trojan Horse 是指(　　)。

A. 病毒　　B. 蠕虫　　C. 特洛伊木马　　D. 漏洞利用程序

2. 恶意软件中，Exploit 是指(　　)。

A. 病毒　　B. 蠕虫　　C. 特洛伊木马　　D. 漏洞利用程序

3. 维持远程控制权类恶意软件的主要目的是(　　)。

A. 保护其他恶意软件　　B. 完成特定业务逻辑

C. 尽力传播恶意软件　　D. 扫描附近其他主机漏洞

4. netstat 命令所带参数“o”的作用是列出(　　)。

A. 相关网络操作进程的输出　　B. 相关网络操作进程的进程 ID

C. 相关网络操作进程的线程输出　　D. 相关网络操作进程的线程数量

5. SQL Injection 是指(　　)。

A. SQL 查询　　B. SQL 漏洞　　C. SQL 注入　　D. 以上都不是

三、 简答题

1. 获取目标系统远程控制权类恶意软件的主要入侵手段有哪些?
2. 第一类恶意软件中，非主动方式感染目标系统的是哪一种？其感染原理是什么？
3. 只观看从网络上的电影绝不会被恶意软件入侵，这个观点是否正确？原因是什么？
4. 简述操作系统补丁、应用软件补丁及时更新的重要性。
5. 简述充分运用最小权限原则，能有效降低恶意软件造成的危害的原理。

第9章　Internet安全协议

前面的章节介绍过密码算法基础、身份认证以及访问控制相关的内容，其中涉及一些认证协议和密钥交换协议，它们都属于安全协议的一小部分。这一章我们将介绍 Internet 安全协议有关的基本概念、安全协议及其特点和不足，使读者能够在实际工作中对已知协议的缺陷和可能受到的攻击采取安全防范措施，加强系统的安全性和稳定性。所谓知己知彼百战百胜，了解既有的网络安全协议和标准，了解对协议进行安全性分析的方法，才能掌握在企业应用中使用这些协议和标准来架构安全的网络应用体系，以期进一步提高在信息安全方面的理论水平和实践能力。

本章重点

- IPSec 协议
- TLS 协议
- Kerberos 协议
- SET 协议

9.1　安全协议概述

所谓协议就是两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。这个定义包含三层含义：

- 协议自始至终是有序的过程，每一个步骤必须执行，在前一步没有执行完成之前，后面的步骤不可能进行。
- 协议至少需要两个参与者。
- 通过协议必须能够完成某项任务。

前面介绍过的密码协议是使用密码学技术的协议，协议的参与者可能是可以信任的人，也可能是攻击者和完全不信任的人。密码协议包含某种密码算法，在网络通信中最常用的、基本的密码协议按照其完成的功能可以分为三类：密码交换协议、认证协议、认证和密钥交换协议。

上述这些协议都属于安全协议的范畴，一个安全协议定义了一个或多个系统的安全。如果将一个计算机系统架设成有一个用来转换状态的转换函数集合组成的有限自动机，那么安全协议有如下的定义。

1. 定义 1

安全协议就是一种状态形式，它把系统的状态分割为一个确定的安全的状态集合与一个不稳定的不安全的状态集合。

2. 定义 2

安全系统就是指系统处在稳定的状态而不能转为不稳定的状态。

3. 定义 3

当系统进入非稳定状态时安全将被破坏。

4. 定义 4

假设 X 表示一个实体集合，I 表示某些信息，那么如果 X 中没有成员包括了关于 I 的信息，则 I 拥有秘密访问 X 的权利。

5. 定义 5

让 X 表示一个实体集合，I 表示某些信息，那么如果 X 中所有成员都信任 I 的信息，则 I 拥有公开访问 X 的权利。

6. 定义 6

让 X 表示为一个实体集合，I 表示某些信息，那么如果 X 中所有成员都能存取 I，则 I 拥有有效的访问 X 的权利。

7. 定义 7

安全手段就是指实施某部分安全协议的实体和步骤。

8. 定义 8

安全模式就是一种提供特殊协议或者协议集的模式。

9. 定义 9

军事安全协议是主要提供机密性的安全协议。

10. 定义 10

商业安全协议是主要提供完整性的安全协议。

11. 定义 11

一个秘密协议是一个只处理秘密性的安全协议。

12. 定义 12

一个完整的协议是一个处理其真实性、完整性的安全协议。

13. 定义 13

一个由开发者控制的存储控制，建立存储由控制(或者是它所拥有的信息)的创造者决定的。

安全协议一般不能有详细的说明，或者说只能是很少的一部分。很明确的安全协议是依赖于它执行的环境。一个经过试验证明的实验，在办公室环境中可能有一个不能改写的协议。一个银行需要一个相当明确的协议，规定各项工作的步骤和部门的职责。

协议的目的就是能遵守条约，而且声明系统管理者和用户都必须遵守法律。这个协议的实施也是有一定的步骤的。对于较小的违约行为，系统可以自我修复。

9.2　IPSec 协议

TCP/IP 的层次不同提供的安全性也不同，例如，在网络层提供虚拟私有网络(VPN)，在传输层提供安全套接服务(Socket)。下面着重介绍在 Internet 层的安全性，即 IPSec 的相关内容。有兴趣的读者可以自行搜索阅读协议标准文档 RFC2401。

9.2.1　IPSec 概述

对 Internet 层的安全协议进行标准化的想法早就有了，在过去的几十年里已经提出了一些方案。例如“安全协议 3 号(SP3)”就是美国国家安全局以及标准技术协会作为“安全数据网络系统(SDNS)”的一部分而制定的。“网络层安全协议(NLSP)”是美国国家科技研究所提出的包括 IP 和 CLNP 在内的统一安全机制。SwIPe 是另一个 Internet 层的安全协议，由 Ioannidis 和 Blaze 提出并实现原型。

所有这些协议的提案的共同点多于不同点，事实上，它们都使用的是 IP 封装技术。其本质是，纯文本的包被加密，封装在外层的 IP 包头里，用来对加密的包进行 Internet 上的路由选择。到达另一端时，外层的 IP 报头被拆开，报文被解密，然后送到接收报文的地点。

Internet 工程特遣组(IETF)特许 Internet 协议安全协议(IPSec)工作组对 IP 安全协议和对应的 Internet 密钥管理协议进行标准化工作。IPSec 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制不仅能在通行的 IP(IPv4)下工作，也能在 IP 的新版本(IPng 或 IPv6)下工作。该体制是与算法无关的，即使替换了加密算法，也不对其他部分的产生影响。按照这个要求，IPSec 工作组制定出了一套规范。

IPSec 被设计成为能够为 IPv4 和 IPv6 提供可交互操作的高质量的基于加密的安全。安全服务集提供包括访问控制、无连接的完整性、数据源认证、抗重播(Replay)保护序列完整性(SequenceIntegrity)的一个组成部分、保密性和有限传输流保密性在内的服务。这些服务是基于 IP 层的，提供对 IP 及其上层协议的保护。

IPSec 为 IP 层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置服务所需密钥到相应位置。IPSec 用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。在 IPSec 文档中，“安全网关”指的是执行 IPSec 协议的中间系统(Intermediate System)。例如，路由器或实现了 IPSec 的防火墙，我们称之为“安

全网关”。

IPSec 能提供的安全服务包括访问控制、无连接的完整性、数据源认证、抗重播(Replay)保护、保密性和有限传输流保密性在内的服务。IPSec DOI 也支持 IP 压缩协议。当在 IPSec 中使用加密而阻碍底层压缩的有效性时，IP 压缩协议被激活。这些算法辅以 IPSec 传输保护和密钥管理协议的使用，为系统和应用开发者采用基于 IP 层的高质量的加密的安全技术提供了途径。

9.2.2　IPSec 安全体系结构

IPSec 实现工作于一个主机或一个安全网关的环境中，对 IP 传输提供保护。所提供的保护是基于：由用户或系统管理员建立和维护的安全策略数据库(SPD)所定义的需求；由用户或系统的管理员建立的具有约束性应用操作所定义的需求。通常，通过基于同数据库(SPD)入口相匹配的 IP 层和传输层头部信息的三种处理模式之一来选择包。每一个包或被给予 IPSec 安全服务或被丢弃或被允许通过 IPSec，这都基于选择符定义的相应数据库策略。

1. IPSec 工作原理

IPSec 使用两个不同的协议——AH 和 ESP 来确保通信的认证、完整性和机密性。它既可以保护整个 IP 数据报，也可以只保护上层协议。

- IP 头部认证(AH)提供无连接的完整性验证、数据源认证、选择性抗重播服务。
- 封装安全负载(ESP)提供加密、有限传输流加密。它也提供无连接的完整性验证、数据源认证、抗重播服务。无论 ESP 什么时间被调用，这些安全服务的某一集合必须被应用。
- AH 和 ESP 均是基于密钥的分布和与这些安全协议相关的传输流管理，AH 和 ESP 均可作为访问控制的媒介物。

这些协议或者独立使用或者组合使用以提供 IPv4 和 IPv6 环境下所需的安全服务集。每个协议支持两种使用模式：传输模式、隧道模式。在隧道模式下，IP 数据报被 IPSec 协议完全加密成新的数据报，并通过隧道传输；在传输模式下，仅仅是有效负荷被 IPSec 协议将 IPSec 头插入 IP 头和上层协议头之间传输，为高层提供基本的保护。

IPSec 允许用户(系统管理员)控制安全服务的粒度(Granularity)。例如，用户可以在两个安全网关间创建单一加密隧道传输所有信息，也可以为每一通过这些网关通讯的主机对的每一个 TCP 连接创建一个独立的加密隧道。

IPSec 管理必须体现下列特性。

- 使用哪些安全服务及在哪种组合中被使用。
- 指定安全保护应该使用的粒度。
- 对基于加密的安全产生影响的算法。

因为这些安全服务使用共享的安全值(密钥)，IPSec 依赖一组独立的机制来存放这些密钥。这些密钥用作认证、完整性验证及加密服务。本文档需要支持手动、自动两种分配方式。它为自动密钥管理定义了一个特殊的基于公共密钥的方法(IKE-[MSST97，Orm97，HC98])，但其他自动密钥分配技术也可以使用。

2. IPSec 实现方式

在主机上或路由器、防火墙(创建安全网关)的连接处，IPSec 可以有几种实现方式。下面提供几个常用的例子。

1) IPSec 完全嵌入原有的 IP 层实现

这种方式涉及 IP 源码，并且对主机和网关都要适用的情况下采用。

2) “Bump-in-the-stack”(BITS)实现

IPSec 实现于原有 IP 协议栈的下部，处于原有的 IP 和网络设备之间。在这种情况下并不需要涉及 IP 协议栈的源码，所以该实现方法适用于遗留系统，大多在主机上采用。

3) 采用外接加密处理设备是军方、金融系统常用的网络安全系统设计方案

这种方式有时被称为“Bump-in-the-wire”(BITW)实现。这种设计方案用于服务主机或者网关，或者两者兼有。通常这种 BITW 设备是可以设定 IP 地址的，当它只支持一个单独的主机的时候，就和 BITS 方案十分相似。但是作为一个支持路由器或防火墙时，它必须实现同一个网关一样的功能并进行相应的操作。

3. 安全连接(Security Association)

安全连接的概念是 IPSec 的基础，是基于 IPv4 和 IPv6 环境下实现 AH、ESP 对安全连接管理的需求。AH 和 ESP 都使用了 SAs，IKE 的主要功能是建立和维护安全连接。所有 AH 和 ESP 的实现都必须支持下面描述的安全连接的概念。接下来将描述安全连接管理的各个方面，定义 SA 策略管理、传输处理、SA 管理技术所需的特性。

1) SA 的定义和范围

安全连接(SA)是一个单向“连接”，它为通过它的传输提供安全服务。SA 通过 AH 或 ESP 但不是两者同时使用而提供安全服务。如果 AH 和 ESP 同时用于传输流的保护，那么应该创建两个或多个 SA 为传输流提供保护。通常为了安全，两台主机间、两个安全网关间或两个安全连接间(每个方向一个)都需要双向通讯。

安全连接由三个部分内容唯一标识——安全参数索引(SPI)、IP 目的地址、安全协议(AH 和 ESP)标识符。原则上，目的地址可以是一个点播地址、IP 广播地址或多播组地址。然而，当前 IPSec SA 管理机制只为点播 SAs 作了定义。因此，在接下来的讨论中，SAs 将只描述点到点通讯的内容，即使这一概念也可以适用点到多的情况。

如上所述我们定义了两种类型的 SAs：传输模式、隧道模式。

传输模式 SA 是两台主机间的安全连接。在 IPv4 环境中，传输模式安全协议头紧接在 IP 头和任何选项之后，在任何更高层协议之前(例如 TCP 或 UDP)。在 IPv6 环境中，安全协议头出现在基本 IP 头和扩展之后，但也许出现在目的选项的前或后，并在更高层协议之前。在采用 ESP 时，传输模式 SA 仅为更高层协议安全服务提供，而不为 IP 头或任何 ESP 头以前的扩展头提供服务。在采用 AH 时，这种保护也被扩展到 IP 头的可选部分、扩展头的可选部分和可选项(包括 IPv4 头、IPv6 Hop-by-Hop 扩展头或 IPv6 目的扩展头)。为了解更多关于 AH 给予的有效区域，请参看 AH 规范。

隧道模式 SA 必然是运用于 IP 隧道的 SA。只要安全连接的任意一端是安全网关，SA 就

必须是隧道模式。因此两个安全网关之间总是隧道模式，同样主机和安全网关间也必然是隧道模式。注意在传输指向安全网关的情况下，例如 SNMP 命令，安全网关是作为主机提供服务的，因而传输模式是被允许的。但在这种情况下，安全网关不再扮演网关的角色，例如它不再转发传输流。两个主机间也可以建立隧道模式 SA。由于为了避免 IPSec 包分段、重组时出现的潜在问题以及这一环境中安全网关后同一目的地存在多重到达路径(例如通过不同的安全网关)，对于任意(转发传输流)SA 包括安全网关都应该可以支持隧道模式。

对于隧道模式 SA，有外部(outer)IP 头、内部(inner)IP 头。外部 IP 头定义了 IPSec 处理的目的地，内部 IP 头定义了包最终地址。安全协议头出现在外部 IP 头后内部 IP 头前。如果在隧道模式中使用 AH，外部 IP 头的部分将受到保护。同样所有隧道化(tunneled)IP 包也受到保护(即所有内部 IP 头、更高层协议受到保护)。如果使用 ESP，则仅对隧道化的包给予保护而不保护外部头。总而言之：

- 主机必须支持传输模式和隧道模式。
- 安全网关仅需要支持隧道模式即可。如果它支持传输模式，仅当安全网关作为主机时使用，例如作为网络管理。

2) 安全连接的功能性

由 SA 提供的安全服务集依赖于安全协议的选择、SA 模式、SA 端点以及在协议范围内可选服务的选择。例如，AH 提供数据源认证和 IP 数据报无连接的完整性验证(以后均称为认证)。准确地讲，认证服务是使用 AH 的安全连接粒度的功能。这将在 4.4.2 节讨论——选择符。

对于分离的接收者，AH 提供抗重播(部分序列完整性)服务以防范拒绝服务的攻击。当不需要保密(或不允许，例如政府限制加密的使用)时，使用 AH 协议是适合的。AH 也为 IP 头可选部分提供认证。这在某些情况下是有必要的。例如，如果在收发双方间，IPv4 选项或 IPv6 扩展头的完整性必须被保护到路由时，AH 能提供这种服务(除了 IP 头不可预料的、易变的部分)。

ESP 可以有选择地为传输提供保密。保密服务的长度部分依赖于所使用的加密算法。ESP 也可以有选择地提供认证服务(正如上面所定义的)。如果一个 ESP SA 认证经过协商，接受方也可以选择具有和 AH 抗重播服务一样特性的增强抗重播服务。由 ESP 提供的认证范围比 AH 所提供的要窄。例如，ESP 头外部的 IP 头就不受保护。如果仅上层协议需要被认证，则最好选择 ESP 认证，并且它具有比使用 AH 封装 ESP 时更高的空间效率。要注意的是尽管保密和认证均是可选的，但是它们不能都被省略。它们中至少有一个必须被选择。

如果选择保密服务，则两个安全网关间的 ESP(隧道模式) SA 能提供局部传输流保密。隧道模式的使用允许内部 IP 头倍加密，隐藏(最终的)传输源和目的的标识。而且也可能调用 ESP 负载填充(ESP Payload Padding)隐藏包的尺寸，甚至隐藏传输的外部特性。在拨号环境下，当一个移动用户被指定一个动态 IP 地址并对一个联合防火墙(Corporate Firewall)建立一个(隧道模式)ESP SA 时，也可以提供类似的传输流保密服务。值得注意的是粒度(Granularity)较精巧的 SAs 通常比那些来自很多用户传输流粒度较粗糙的 SAs 更容易受到传输分析。

3) 安全连接的组合

通过独立 SA 的 IP 数据报通过严密的安全协议(AH 或 ESP)受到保护。对于特殊的传输

流，而仅采用单一的 SA 是不能实现的。在这种情况下，使用多重 SAs 以实现安全策略是必要的。术语"安全连接束"或"SA 束"定义为一个 SAs 序列(Sequence)，传输必须通过它来满足一个安全策略，策略定义了序列的顺序。值得注意的是由束组成的 SAs 可能终止于不同的端点。例如，一个 SA 可以在移动主机、网关和另一个网关之间延展，嵌套的 SA 可以延展到网关后的主机。

安全连接可以通过两种方式组合成束：传输邻接(Transport Adjacency)和隧道迭代(Iterated Tunneling)。

- 传输邻接指的是对同一个 IP 报文使用多于一个安全协议，而不采用隧道方式。这种联合 AH 和 ESP 的方法只允许一级联合；更多的嵌套并不能增加效益(假设每一个协议中使用了足够强壮的算法)，因为这一过程仅被执行于 IPsec 最终目的地的 IP 实例处，如图 9-1 所示。

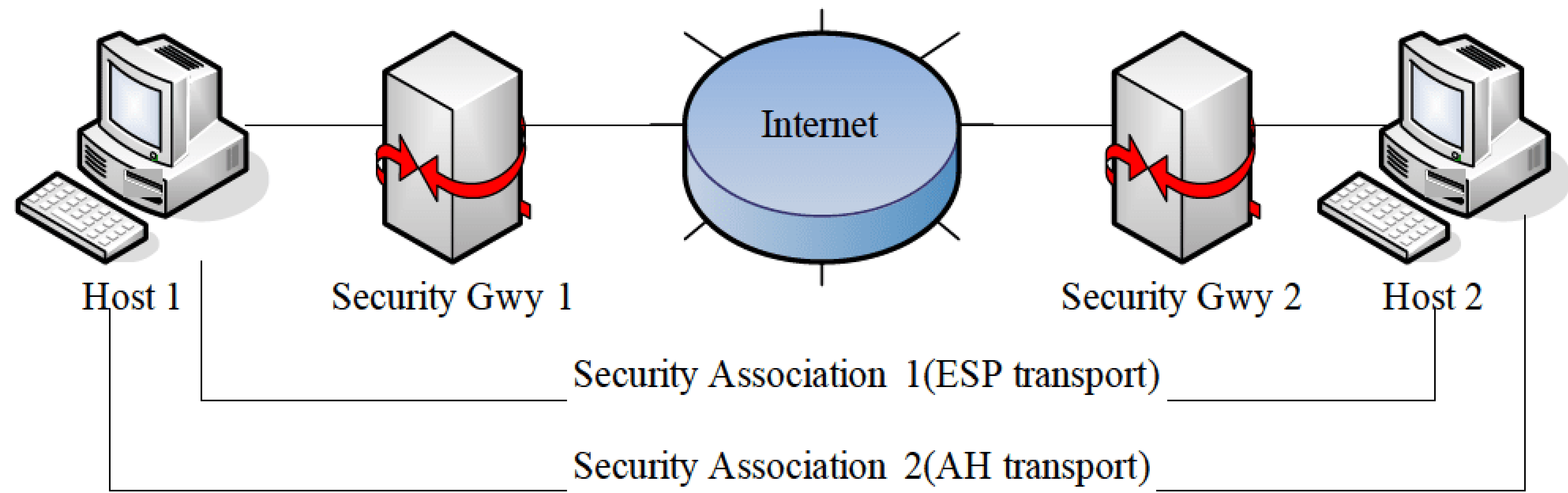


图 9-1　传输邻接示意图

- 隧道迭代指的是一种对安全协议的多层次应用，这一安全协议是通过 IP 隧道实现的。这种方法允许多重叠代，这是因为每一个隧道可能沿着一路径在不同的 IPSec 站点(IPSec site)开始、结束。除了那些能通过合适的 SPD 入口被定义的以外，在中间安全网关处对于 ISAKMP 传输不希望采用特殊的处理。

有三种基本的隧道迭代情况，仅情况后两种情况需要支持。

- 对于 SAs 两个端点都是同样的——内部隧道和外部隧道采用 AH 或 ESP，但主机 1 几乎不可能把两个指定成一样。即 AH 的内部不可能是 AH，ESP 的内部不可能是 ESP，如图 9-2 所示。

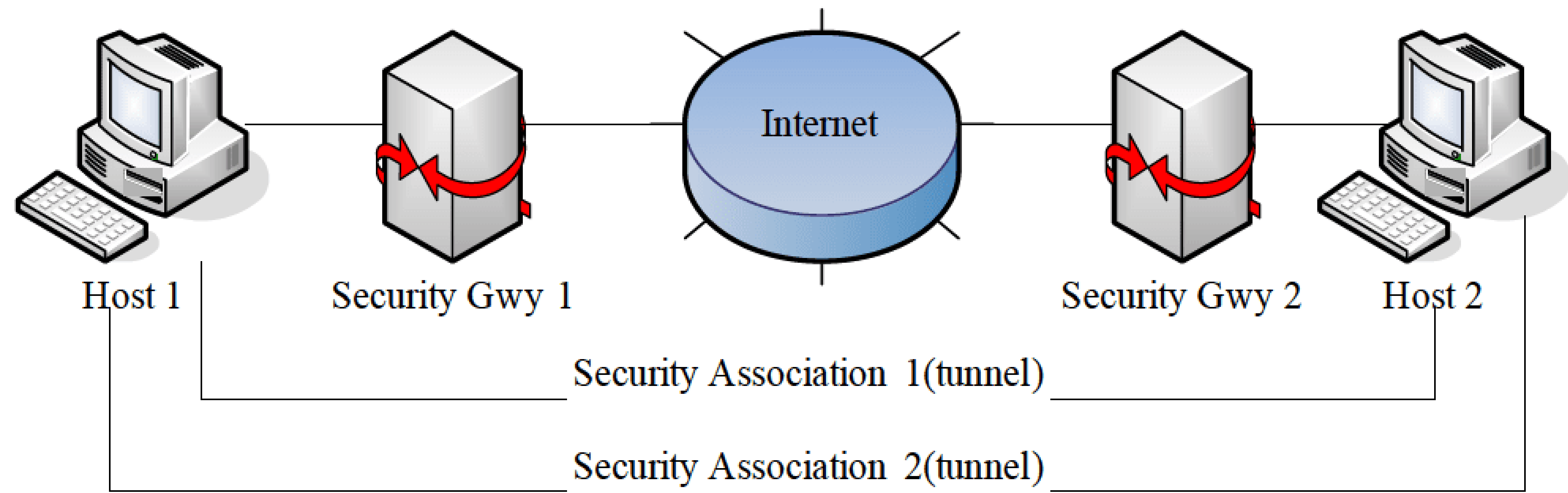


图 9-2　第一种隧道迭代

- 对于 SAs 一个端点是一样的——内部隧道和外部隧道采用 AH 或 ESP，如图 9-3 所示。

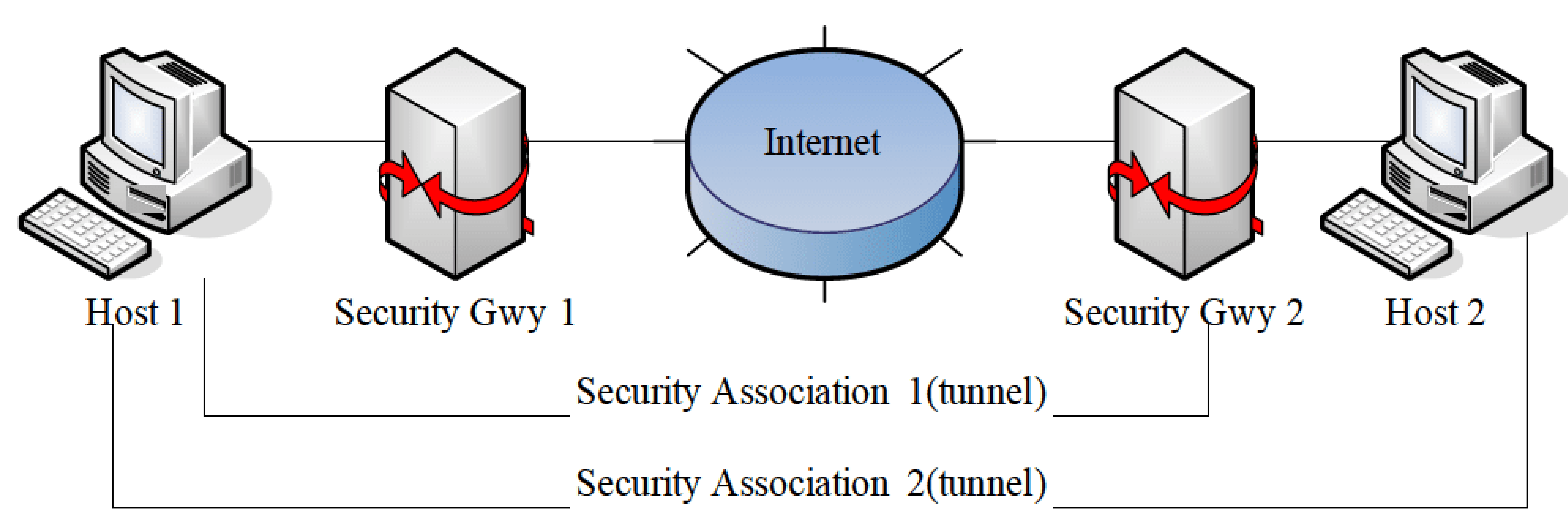


图 9-3　第二种隧道迭代

- 任意一个端点都不同——内部隧道和外部隧道采用 AH 或 ESP，如图 9-4 所示。

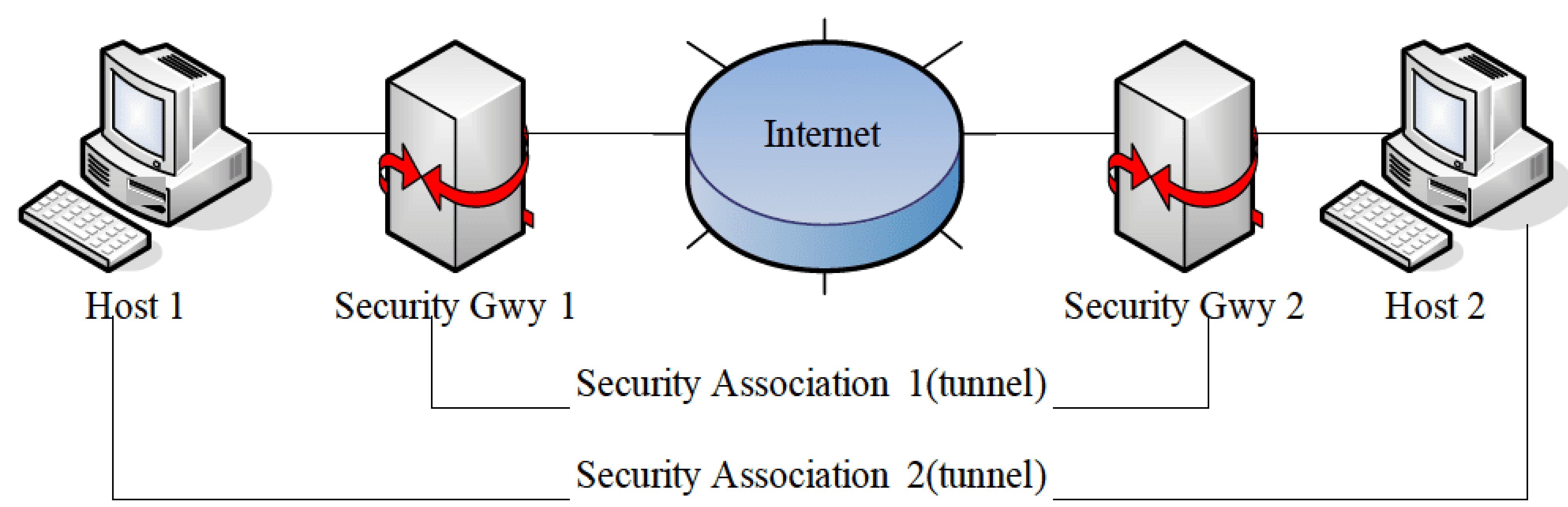


图 9-4　第三种隧道迭代

这两种方式也可以被组合。例如，一个 SA 束能由一个隧道模式 SA 和一个或两个传输模式 SAs 构成应用于序列。值得注意的是嵌套的隧道也能发生在任何隧道源或目的端点都不相同的地方。在这种情况下，没有与嵌套隧道相关的带有束的主机或网关存在。

对于传输模式 SAs，只有一个安全协议序是合适的。

4) 安全连接数据库

为保护 IP 数据报的完整性，IPSec 协议使用了散列信息认证代码(Hash Message Authentication Codes，HMAC)。为了得到这个“散列信息认证代码”，IPSec 使用了像 MD5 和 SHA 这样的散列算法根据一个密钥和数据报的内容来生成一个“散列”。这个“散列信息认证代码”包含在 IPSec 协议头并且数据包接受者可以检查“散列信息认证代码”(当然前提是可以访问密钥)。

为了保证数据报的机密性，IPSec 协议使用对称加密算法。IPSec 标准需要 NULL 和 DES 执行者。如今经常使用像 3DES、AES 和 Blowfish 这样更加强的算法。

通信的双方为了能够加密和解密 IPSec 数据包，它们需要一种方法来保存通信的密钥、算法和 IP 地址等有关信息。所有这些用来保护 IP 数据报的参数保存在 SA(Security Association，SA)中。SA 依次保存在 SA 数据库(Security Association Database，SAD)中。

SA 仅仅声明 IPSec 支持保护通信。需要定义另外的信息来声明什么时候通信需要保护。这些信息保存在安全策略(Security Policy，SP)中，安全策略又依次保存在安全策略库(Security Policy Database，SPD)中。“安全策略”通常声明下列参数。

- 被保护的数据包的源地址和目标地址。在传输模式下，这同 SA 的地址相同。在隧道模式下，它们可能不一样。

- 被保护的协议和端口。一些 IPSec 执行者不允许定义被保护的协议，这种情况下将保护所有涉及的 IP 地址之间的通信。
- 用来保护数据包的 SA。

根本上，安全连接是一个用来在 IPSec 环境中增加安全策略的管理结构。因此 SA 处理必不可少的元素是一个下层的安全策略数据库，它定义哪些服务将被提供给 IP 数据报，用什么方式把哪些服务提供给 IP 数据报。在所有的过程中，必须考虑 SPD。

SPD 必须区分受 IPSec 保护的传输和允许通过 IPsec 的传输。这运用于由发送者使用的 IPSec 保护和必须有接收者参与的 IPSec 保护。对于任何输出或输入的数据报有三种可能的选择：丢弃、穿过 IPSec 或使用 IPSec。第一种选择是指根本不允许退出主机、穿过安全网关，或最终传递到某一应用程序。第二种选择指的是允许通过而不用额外 IPsec 保护的传输。第三种选择指的是需要 IPSec 保护的传输并且对于这样的传输 SPD 必须规定提供的安全服务，所使用的协议、算法等。

SPD 包括策略的有序列表。每一个策略由一个或多个选择符标识，这些选择符定义了被这一策略包含的 IP 传输。

密钥和加密算法必须被共享到所有 VPN(Virtual Private Network)双方。特别是交换密钥给系统管理员造成危险的问题：在没有加密的情况下如何交换对称的密钥？

为了解决这个问题，又发明了互联网密钥交换(Internet Key Exchange，IKE)协议。这个协议在通信的第一阶段鉴定双方身份。在第二阶段，商议好 SA 并且对称密钥改变成使用一种 Diffie Hellmann 密钥交换，然后互联网密钥交换协议周期性地改变密钥来确保它们的机密性。

9.2.3　认证头协议

如前文所述，IPSec 协议包括两个协议：认证头协议(Authentication Header，AH)和安全负载封装协议(Encapsulated Security Payload，ESP)，两者都独立于 IP 协议。认证头协议使用 IP 协议 51，封装安全负载协议使用 IP 协议 50。定义 AH 认证头协议的标准是 RFC2402。

认证头协议保护 IP 双数据报的完整性。为了达到这一点，认证头协议计算了一个散列信息认证代码(HMAC)来保护完整性。

如图 9-5 所示，认证头共 24 个字节长。第一个字节是“下一个头”字段，这个字段指定了下边协议的头。在隧道模式下，一个完整的 IP 数据报被封装，因此这个字段的值是 4。在传送模式下，当被封装的是 TCP 数据报时相应的值是 6。下一个字节指定了有效负载的长度。这个字段下边是两个保留字节。再下边两个双节指定了 32 位长的安全参数索引(Security Parameter Index，SPI)。安全参数索引指定了解安全负载封装使用的 SA。32 位长的序号防止重复攻击。最后 96 位保存了散列信息认证代码(HMAC)。散列信息认证代码保护了数据包的完整性，因为只有双方知道可以创建和检查散列信息认证代码的密钥。

8	16	32bit
Next Header	Payload Length	Reserved
Security parameters index (SPI)		
Sequence Number Field		
Authentication data (variable)		

图 9-5　AH 数据格式

9.2.4　安全负载封装协议

定义安全负载封装协议(Encapsulated Security Payload，ESP)的标准是 RFC2406。

安全负载封装协议既可以使用散列信息认证代码来确保数据包的完整性，又可以使用加密算法保证机密性。在加密数据包并计算出散列信息认证代码后，生成安全负载封装头并加入数据包。安全负载封装头包括两部分，如图 9-6 所示。

16	24	32bit
Security association identifier (SPI)		
Sequence Number		
Payload data (variable length)		
Padding (0-255 bytes)		
	Pad Length	Next Header
Authentication Data (variable)		

图 9-6　ESP 数据格式

安全负载封装头的第一个双字字段指定了安全参数索引(SPI)，这个“索引”指定了解安全负载封装数据包用到的“SA”。下一个双字字段保存序号，序号被用来预防重复攻击。第三个双字字段指定了加密程序使用的初始向量(Initialization Vector，IV)。不使用初始向量对称加密算法可能被多次攻击。初始向量可以确保两个相同的负载被加密成不同的负载。

IPSec 使用密码块来进行加密处理。因此，如果负载的长度不是声的整倍长时可能需要填补，这时需要增加填补长度。下边的两个字节是填补长度。下一个头字段指定了下一个头。安全负载封装头的最后 96 位长是散列信息认证代码，用来确保数据包的完整性。这个散列信息认证代码仅仅统计数据包的负载。IP 头不包括在计算之列。

因此，使用网络地址转换不会破坏安全负载封装协议。尽管如此，大多数情况下网络地址转换不可能与 IPSec 结合。在这种情况下，横越网络地址转换(NAT-Travesal)提供了一个解决办法——把安全负载封装数据包封装到 UDP 数据包中。

9.2.5　因特网密钥交换协议

因特网密钥交换协议(IKE Protocol)解决了安全通信设备中的大多数突出问题：确认双方并交换双称密钥。它创建 SA 并装入 SA 数据库中。因特网密钥交换协议经常需要一个用户空间守护进程并且不在操作系统核心中执行。因特网密钥交换协议使用 UDP 的 500 端口来进行通信。

因特网密钥交换协议功能分两个阶段。第一阶段建立一个因特网 SA 密钥管理 SA(Internet Security Association Key Management Security Association，ISAKMP SA)；第二阶段，因特网 SA 密钥管理 SA 用来商讨并配置 IPSec 的 SA。

双方的第一阶段认证经常使用基于预先共享密钥(Pre-Shared Keys，PSK)、RSA 密钥(RSA Keys)和 X.509 证书(Racoon 甚至支持 Kerberos)。

第一阶段通常支持两种不同的模式：主模式和好斗模式。两种模式都鉴别对方并设置 ISAKMP SA，但好斗模式只使用一半数量的信息达到这个目。这是它的缺点，因为好斗模块不支持身份保护，因此如果与预共享密钥一起使用，它容易受到“中间人攻击”(Man-in-the-middle Attack)。另一方面，这只是好斗模式的用途，因为主模式的内部工作形式不支持对未知的一方使用不同的预共享密钥。好斗模式不支持身份保护和用普通文字传送客户的身份，因此在认证发生前，一方知道另一方，并且不同的预共享密钥可以被不同的一方使用。

在第二阶段，IKE 协议交换 SA 建议(Security Association Proposal)并且基于 ISAKMP SA 商议的 SA。ISAKMP SA 提供认证来避免中间人攻击(Man-in-the-middle Attack)。第二阶段使用快速模式。

9.3　TLS

安全传输层协议(Transport Layer Security Protocol，TLS)用于在两个通信应用程序之间提供保密性和数据完整性。

1997 年，IETF 基于 SSLv3 协议发布了 TLS(Transport Layer Security)v1 传输层安全协议的草案。1999 年，正式发布了 RFC2246。TLSv1 成为工业标准以后，不久 TLSv1 在因特网上也得到了广泛的应用。除了如 S / HTTP、S / MIME、SSL-Telnet、SSL-SMTP 和 SSL-POP3 等常用的协议以外，目前许多电子商务和电子政务系统也基于 TLS 来确保其安全性。

9.3.1　TLS 概述

TLS 设计的具体目标是解决两个通信实体之间的数据保密性和完整性等，总体目标是为了在因特网上统一 SSL 的标准。因此，在协议构成方面，TLS 几乎与 SSL 协议一样，主要分为 TLS 记录协议与 TLS 握手协议。TLS 记录协议与 SSL 记录协议基本一致，字段的内容也基本相同。TLS 记录协议也有 4 种类型的客户：握手协议、警告协议、改变密码规格协议和应用数据协议等。为了便于 TLS 的扩展，TLS 记录协议还支持额外的记录类型。

9.3.2　TLS 工作原理

该协议由两层组成：TLS 记录协议(TLS Record)和 TLS 握手协议(TLS Handshake)。较低的层为 TLS 记录协议，位于某个可靠的传输协议(例如 TCP)上面。

TLS 协议包括两个协议组：TLS 记录协议和 TLS 握手协议，每组具有很多不同格式的信息。限于篇幅，在此我们只列出协议摘要但不作具体解析，具体内容可参照协议相关文档。

TLS 记录协议是一种分层协议。每一层中的信息可能包含长度、描述和内容等字段。记录协议支持信息传输、将数据分段到可处理块、压缩数据、应用 MAC、加密以及传输结果等。对接收到的数据进行解密、校验、解压缩、重组等，然后将它们传送到高层客户机。

TLS 连接状态指的是 TLS 记录协议的操作环境，它规定了压缩算法、加密算法和 MAC 算法。

TLS 记录层从高层接收任意大小无空块的连续数据。密钥计算：记录协议通过算法从握手协议提供的安全参数中产生密钥、IV 和 MAC 密钥。TLS 握手协议由三个子协议组构成，允许对等双方在记录层的安全参数上达成一致、自我认证、例示协商安全参数、互相报告出错条件。

TLS 建立会话协商的参数、握手协议过程等与 SSL 一致，其基本的工作流程分为如下两个阶段。

1. 服务器认证阶段

(1) 客户端向服务器发送一个开始信息“Hello”，以便开始一个新的会话连接。

(2) 服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息。

(3) 客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器。

(4) 服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

2. 用户认证阶段

在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回(数字)签名后的提问和其公开密钥，从而向服务器提供认证。

9.3.3 TLS 的安全服务

TLS 是在网络传输层上提供的一种用于网络实体之间安全数据传输的协议，使用了 RSA、DES 等多种加密算法。向上层应用提供三种基本的安全性服务，每一种都包含了公共密钥技术。

1. 保密性

通过公共密钥和秘密密钥加密的组合实现，在服务器和客户之间的所有通信都通过一个密钥和一个协商好的加密算法进行加密。加密方法的协商是在握手期间完成的。

2. 完整性

TLS 使用秘密共享和 Hash 函数进行 MAC 计算来提供信息的完整性服务。

3. 不可抵赖性

TLS 以公共密钥凭证的形式对身份进行编码，在握手过程中相互交换以互相认证。

TLS 记录协议提供的连接安全性具有两个基本特性。

- 私有：对称加密用以数据加密(DES、RC4 等)。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议(如握手协议)协商。
- 可靠：信息传输包括使用密钥的 MAC 进行信息完整性检查，安全哈希功能(SHA、MD5 等)用于 MAC 计算。

9.3.4　TLS 的特点与不足

TLS 用于封装各种高层协议。作为这种封装协议之一的握手协议允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间相互认证，协商加密算法和加密密钥。TLS 握手协议提供的连接安全具有三个基本属性。

- 可以使用非对称的或公共密钥的密码术来认证对等方的身份。该认证是可选的，但至少需要一个结点方。
- 共享加密密钥的协商是安全的，对偷窃者来说，协商加密是难以获得的。此外经过认证过的连接不能获得加密，即使是进入连接中间的攻击者也不能。
- 协商是可靠的。没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

TLS 的最大优势在于：TLS 是独立于应用协议。高层协议可以透明地分布在 TLS 协议上面。然而，TLS 标准并没有规定应用程序如何在 TLS 上增加安全性；它把如何启动 TLS 握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

9.4　Kerberos 协议

Kerberos 协议主要用于计算机网络的身份认证(Authentication)，其特点是用户只需输入一次身份验证信息就可以凭借此验证获得的票据(Ticket-Granting Ticket)访问多个服务，即 SSO(Single Sign On)。由于在每个 Client 和 Server 之间建立了共享密钥，使得该协议具有相当的安全性。

9.4.1　Kerberos 概述

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下，Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术(如：共享密钥)执行认证服务的。

9.4.2　Kerberos 工作原理

具体的认证过程如下：客户机向认证服务器(AS)发送请求，要求得到某服务器的证书，

然后 AS 的响应包含这些用客户端密钥加密的证书。证书的构成为：服务器“Ticket”；一个临时加密密钥(又称为会话密钥“Session Key”)。客户机将 Ticket (包括用服务器密钥加密的客户机身份和一份会话密钥的副本)传送到服务器上。会话密钥可以(现已经由客户机和服务器共享)用来认证客户机或认证服务器，也可用来为通信双方以后的通信提供加密服务，或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。

上述认证交换过程需要只读方式访问 Kerberos 数据库。但有时，数据库中的记录必须进行修改，如添加新的规则或改变规则密钥时。修改过程通过客户机和第三方 Kerberos 服务器(Kerberos 管理器 KADM)间的协议完成，有关管理协议在此不作介绍。另外也有一种协议用于维护多份 Kerberos 数据库的拷贝，这可以认为是执行过程中的细节问题，并且会不断改变以适应各种不同的数据库技术。

下面以图示方式简单说明 Kerberos 的相关原理。首先，看一下 Kerberos 协议的前提条件，如图 9-7 所示，Client 与 KDC，KDC 与 Service 在协议工作前已经有了各自的共享密钥。

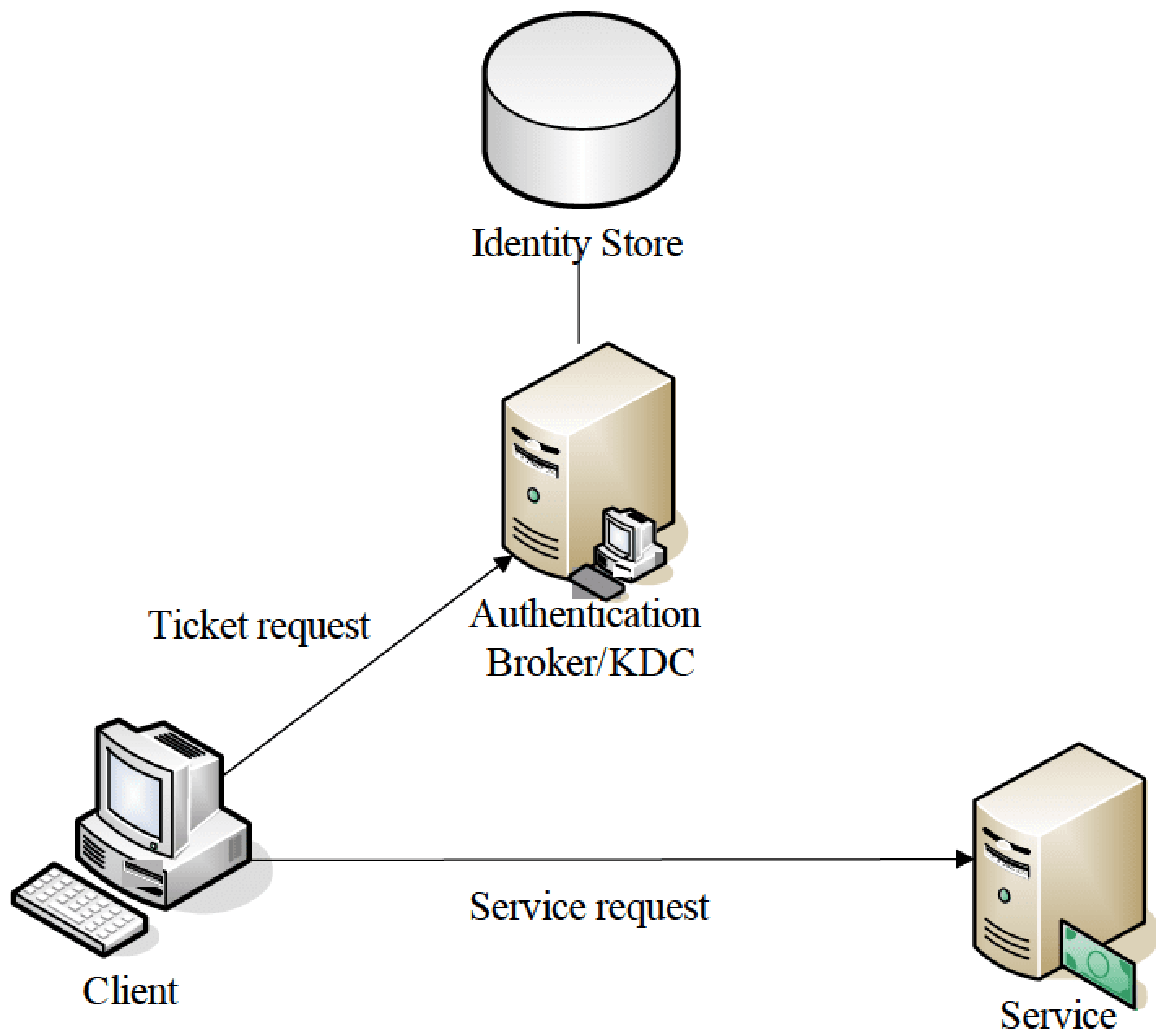


图 9-7　Client，KDC，Service 关系

Kerberos 协议分为两个部分。

- Client 向 KDC 发送自己的身份信息，KDC 从 Ticket Granting Service 得到 TGT(Ticket-Granting Ticket)，并用协议开始前的密钥将 TGT 加密回复给 Client。

此时只有真正的 Client 才能利用它与 KDC 之间的密钥将加密后的 TGT 解密，从而获得 TGT。此过程避免了 Client 直接向 KDC 发送密码，以求通过验证的不安全方式。

- Client 利用之前获得的 TGT 向 KDC 请求其他 Service 的 Ticket。

Kerberos 协议的重点在于第二部分，如图 9-8 所示。

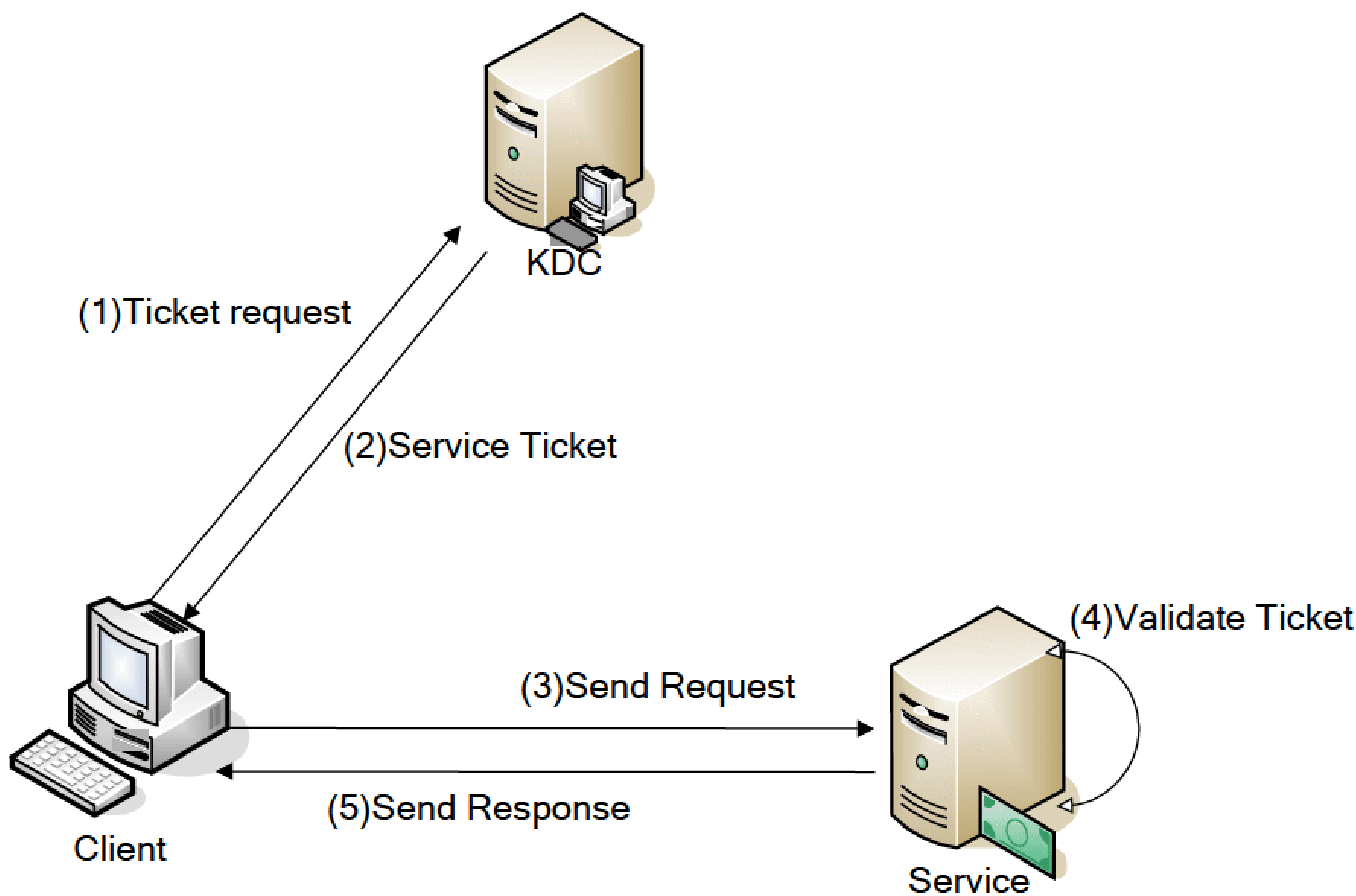


图 9-8 认证过程

(1) Client 将之前获得 TGT 和要请求的服务信息(服务名等)发送给 KDC，KDC 中的 Ticket Granting Service 将为 Client 和 Service 之间生成一个 Session Key，用于 Service 对 Client 的身份鉴别。然后 KDC 将这个 Session Key 和用户名、用户地址(IP)、服务名、有效期、时间戳一起包装成一个 Ticket(这些信息最终用于 Service 对 Client 的身份鉴别)发送给 Service。

(2) 此时 KDC 将刚才的 Ticket 转发给 Client。由于这个 Ticket 是要给 Service 的，不能让 Client 看到，所以 KDC 用协议开始前 KDC 与 Service 之间的密钥将 Ticket 加密后再发送给 Client。同时为了让 Client 和 Service 之间共享那个秘密(KDC 在第一步为它们创建的 Session Key)，KDC 用 Client 与它之间的密钥将 Session Key 加密，然后随加密的 Ticket 一起返回给 Client。

(3) 为了完成 Ticket 的传递，Client 将刚才收到的 Ticket 转发到 Service。由于 Client 不知道 KDC 与 Service 之间的密钥，所以它无法更改 Ticket 中的信息。同时 Client 将收到的 Session Key 解密出来，然后将自己的用户名、用户地址(IP)打包成 Authenticator，然后用 Session Key 加密也发送给 Service。

(4) Service 收到 Ticket 后利用它与 KDC 之间的密钥将 Ticket 中的信息解密出来，从而获得 Session Key 和用户名、用户地址(IP)、服务名、有效期。然后再用 Session Key 将 Authenticator 解密，从而获得用户名、用户地址(IP)，之后将其与之前 Ticket 中解密出来的用户名、用户地址(IP)做比较从而验证 Client 的身份。

(5) 如果 Service 有返回结果，将其返回给 Client。

9.4.3 Kerberos 的安全服务

从上面描述的流程来看，Kerberos 协议主要完成了两件事，概括起来就是提供了如下的安全服务。

1. 保密性

完成 Ticket 的安全传递。

2. 完整性

完成了 Session Key 的安全发布。再加上时间戳，在很大程度上保证了用户鉴别的安全性，并且利用了 Session Key，通过鉴别之后 Client 和 Service 之间传递的消息也可以获得一定的机密性(Confidentiality)、完整性(Integrity)的保障。

9.4.4 Kerberos 的特点与不足

如前面所介绍的，由于 Kerberos 协议的消息无法穿透防火墙，因此限制了该协议往往应用于一个组织内部，这一点使得它的应用范围受到一定的局限。

另外，由于没有使用非对称密钥自然也就无法具有抗否认性，这也限制了它的应用。不过，有失必有得。相对而言，它比 X.509 PKI 的身份鉴别方式实施起来要简单得多。是用实施复杂程度降低换取性能上的缺失，还是用复杂的实施方式获取更高的安全性，是留待用户自行决定的一个问题。

9.5 SET 协议

电子商务的关键是要保证商业活动的安全性，即像传统方法一样安全可靠。而数据加密技术则构成了电子商务安全的基础，可以说，没有数据加密技术，就没有电子商务的安全。电子商务主要有下面一些安全控制要求。

- 确定贸易伙伴身份的真实性。
- 确保信息的保密性，如保证用户的信用卡号不被窃取，保证货源订单等信息不被竞争对手获悉等。
- 保证电子订单等信息的真实性(未被冒充)以及在传输过程中未被篡改。
- 保证电子订单等信息的不可否认性，即交易的任何一方在未经对方同意的情况下都不能出尔反尔。
- 在交易双方发生纠纷时能得到合理的仲裁和解决。

从上面介绍的 SSL 协议可以看出，SSL 协议的基础是商家对消费者信息保密的承诺，有利于商家而不利于消费者。虽然在 SSL 3.0 中通过数字签名和数字证书可实现双方的身份验证，但是 SSL 协议仍存在一些问题，在涉及多方的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。在这种情况下，Visa 和 MasterCard 两大信用卡组织制定了 SET 协议，为网上信用卡支付提供了全球性的标准。

9.5.1 SET 概述

1996 年 2 月，由 VISA 和 MasterCard 两大信用卡公司提出了 SET(Secure Electronic Transaction)协议，该协议是在因特网环境中解决用户、商家和银行之间通过信用卡支付交易而设计的安全规范，获得了诸如 Microsoft、IBM 等许多大公司的支持。SET 是目前唯一保证信用卡信息能安全可靠地通过因特网传输的新协议。

SET 是因特网电子交易中的一组安全规范。采用 SET 协议进行网上交易支付时，主要涉及持卡人、商家、支付网关、发卡人、支付者和 CA 认证中心等，如图 9-9 所示。

- 持卡人，即消费者，他们通过 Web 浏览器或客户端软件购物。
- 商家，在 Internet 上提供在线商店。
- 发卡人，通常为银行，为持卡人开设账户，并且发放用于网上支付的信用卡。
- 支付者，通常为银行，为商家建立账户，并且处理支付卡的认证和支付事务。
- 支付网关，实现对支付信息从 Internet 到银行内部网络的转换，用来处理商家支付报文和持卡人的支付指令，并对商家和持卡人进行身份认证。

认证机构(CA)为电子交易参与方颁发证书，提供权威身份证明。

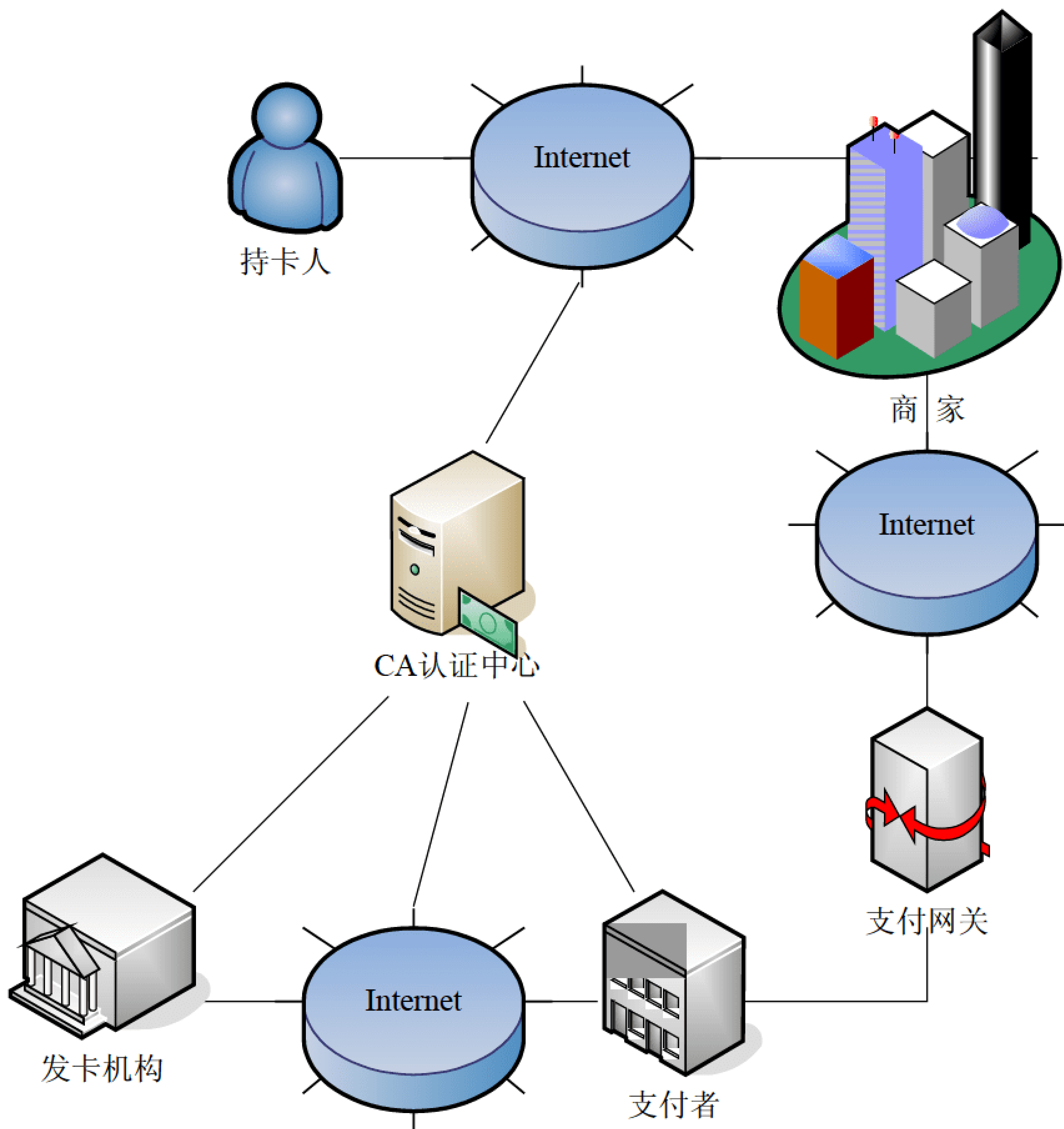


图 9-9　SET 模型

9.5.2　SET 工作过程

在进行 SET 交易之前，消费者首先需要向支持 SET 的银行申请开户，获得一个用于网上支付的信用卡账户。同时，消费者和商家还必须从 CA 认证中心那里申请相应的 X.509 数字证书。此后，商家就可以在因特网上开设超市，持卡人(消费者)也就可以通过浏览器在因特网实现购物。具体的步骤如下所述。

1. 订购商品

- 持卡人通过网上商店浏览商家的商品，选好后在线支付，向商家发送初始请求。

- 商家接受请求，产生初始应答，对初始应答生成消息摘要，对摘要进行数字签名，然后将数字签名等发送给持卡人。

2. 购买商品

- 验证商家。持卡人收到商家的初始应答，验证商家证书和支付网关证书，并利用商家公钥验证消息摘要的数字签名，证实数据在途中未被篡改。
- 发送订单。包括发往商家的订单指令以及通过商家转发给支付网关的支付指令，利用双重签名将和结合起来。

3. 处理订单

- 商家接受持卡人的购物请求，认证持卡人的证书，验证双重签名。
- 支付请求。商家随机产生一个对称密钥为支付请求加密并签名，利用支付网关公钥加密该对称密钥形成数字信封，然后将信息一并发往支付网关。

4. 支付

- 支付网关首先验证商家的证书，利用自己的私钥打开商家数字信封，获取商家的对称密钥，解开支付请求密文，并验证商家支付请求消息的完整性。
- 支付网关验证持卡人的证书，利用私钥打开持卡人的数字信封，得到持卡人的账号和对称密钥，还原出支付指令，然后验证双重签名以及相关消息的完整性等。
- 如果所有验证通过，则生成相应的扣款请求信息，并将该扣款信息发送给相应银行。
- 银行向支付网关发送扣款应答。
- 支付网关在接受银行的扣款应答后，向商家发送支付应答，利用消息摘要、数字签名和数字信封等技术确保支付应答消息的安全性。

5. 购物应答

- 商家接受并检查支付网关的支付应答(包括支付网关的身份验证、消息完整性验证等)，如无误，向持卡人发送购物应答。如果交易成功，则发货。
- 持卡人接受购物应答，并对相关安全性验证，确认交易成功。

9.5.3　SET 的安全功能

SET 协议的安全措施十分完善，它把对称密钥体制和公开密钥体制完美地结合起来，利用数字信封技术进行密钥的安全可靠交换，通过 DES、RSA 等进行高效率数据加密，利用数字证书、消息摘要、时间戳、数字签名和双重签名等技术确保信息的完整性和不可抵赖性等，具有安全性高、密钥管理简便等优点。

数字签名在 SET 协议中的一个重要应用就是双重签名。在交易中持卡人发往银行的支付指令是通过商家转发的，为了避免在交易过程中商家窃取持卡人的信用卡信息，以及避免银行跟踪持卡人的行为，侵犯消费者隐私，但同时又不影响商家和银行对持卡人所发信息进行合理的验证，只有当商家同意持卡人的购买请求后，才会让银行给商家付费。SET 协议采用

双重签名来解决这一问题。

假设持卡人 C(Customer)从商家 M(Merchant)购买商品，他不希望商家看到他的信用卡信息，也不希望银行(Bank)看到他有关商品的信息，于是他采用双重签名，流程如图 9-10 所示，具体说明如下。

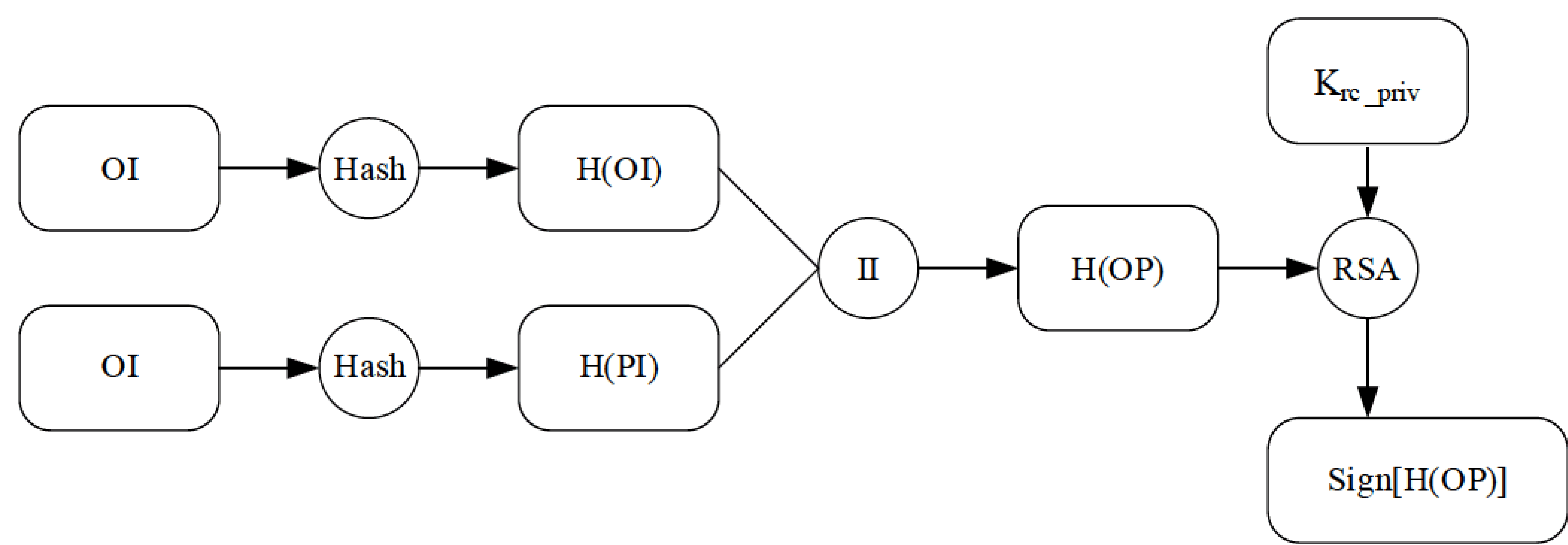


图 9-10 SET 双重签名

首先 C 产生发往 M 的订购信息 OI 和发往 B 的支付指令 n，并分别产生 OI、PI 的摘要 H(OI)，H(PI)，其中摘要由一个单向 Hash 函数产生。连接 H(OI)和 H(PI)得到 OP，再生成 OP 的摘要 H(OP)，用 C 的 RSA 私钥 K_{rc_priv} 签名 H(OP)，得到 sign[H(OP)]，称为双重签名。

然后，C 将消息{OI，H(PI)，sign[H(OP)]}发给 M，将{PI，H(OI)，sign[H(OP)]}}发给 B。在验证双重签名时，接受者 M/B 分别创建消息摘要，M 生成 H(OI)，B 生成 H(PI)，再分别将 H(OI)/H(PI)与另一接收到的摘要 H(PI)/H(OI)连接，生成 OP 及其摘要 H(OP)，接收者 M/B 用 C 的 RSA 公钥 K_{rc_pub} 解开 sign[H(OP)]，得到 H(OP)，比较 H(OP)与 H(OP)是否相同。如果相同，则表示数据完整且未被篡改。

9.5.4 SET 与 TLS 协议的比较

SET 与 TLS 同样提供了电子安全交易的机制，但是运行方式有所差别。

(1) SET 是一个多方的报文协议，它定义了银行、商店和消费者之间必需遵守的报文规范；TLS 只是简单地在交易双方之间建立了安全连接。

(2) TLS 是面向连接的；而 SET 允许各方之间的报文交换不是实时的。

(3) SET 报文能够在银行内部网或者其他网络上传输；而 TLS 之上的交付系统只能与 Web 浏览器捆绑在一起工作。

(4) SET 的安全需求较高，因此所有参与 SET 交易的成员(消费者、商店、支付网关等)都必须先申请数字证书来识别身份，并且整个交易过程都受到严密的保护；而在 TLS 中只有商店端的服务器需要认证，客户端认证是可选的，同时交易过程中的安全范围只限于消费者到商店的信息交换。

(5) SET 交易，除了申请数字证书之外，还必须安装符合 SET 规范的电子钱包软件；而 TLS 交易不需要。

(6) 由于 SET 的成本较高，并且引入中国的时间较短，目前 TLS 的普及率仍较高，大约有七八成，但是网上交易的安全性需求不断提高，可以预料 SET 将会成为日后市场的主流。

本 章 小 结

本章主要介绍了网络安全协议的基本知识，包括网络安全协议概述、IPSec 协议、TLS 协议、Kerberos 协议、SET 协议的相关内容和工作原理；从安全服务的角度出发，评价了各种协议在相关应用方面的优势和不足，并进行了 TLS 和 SET 的比较。希望读者通过本章的学习能够掌握基础的网络安全协议知识，理解 Kerberos、IPSec、SET 协议的内容和实施技术，能够在实践中熟练运用上述协议构建信息安全的企业应用，同时为后面章节的学习打下坚实的基础。

课 后 练 习

一、填空题

1. IPSec、NLSP、SwIPe 的共同点是都采用了(　　　　　)技术。
2. IPSec 使用两个不同的协议(　　　　　)、(　　　　　)来确保通信的认证、(　　　　　)性和(　　　　　)性。
3. IKE Protocol 使用(　　　　　)的端口(　　　　　)进行通信。Kerberos 协议主要用于计算机网络的(　　　　　)，在(　　　　　)和(　　　　　)之间建立共享密钥，使得该协议具有很高的安全性。
4. TLS 与 SET 的区别体现在 TLS 是面向(　　　　　)的，而 SET 允许各方之间的报文交换不是实时的。

二、选择题

1. IPSec 提供的服务都基于(　　)层，所以可以供高层协议使用，例如(　　)。
   A. TCP　　B. IP　　C. UDP　　D. ICMP
2. IPSec 的 AH 协议提供(　　)服务。
   A. 加密　　B. 无连接的完整性验证
   C. 数据源认证　　D. 选择性抗重播
3. IPSec 的 ESP 协议提供(　　)服务。
   A. 加密　　B. 无连接的完整性验证
   C. 数据源认证　　D. 选择性抗重播
4. TLS 协议由(　　)和(　　)两层协议组成。
   A. 记录协议　　B. TCP　　C. UDP　　D. 握手协议
5. 下列功能中，属于 Kerberos 实现的是(　　)。
   A. Session key 安全发布　　B. 安全传递 Ticket
   C. 穿透防火墙　　D. 不可抵赖性

三、 简答题

1. 什么是 IP 封装技术？
2. 列举几种 IPSec 的实现方式，并介绍其特点。
3. 简述 IKE Protocol 的工作原理。
4. 简述 Kerberos 的特点与不足。
5. SET 与 TLS 协议有什么区别？

第10章　公钥基础设施——PKI

公钥基础设施(Public Key Infrastructure，PKI)是一个用于非对称密码算法原理和技术实现，并提供安全服务的具有通用性的安全基础设施。用户利用PKI平台提供的安全服务进行安全通信。PKI是一种遵循标准的密钥管理平台，能为所有网络应用透明地提供采用加密和数字签名等密码服务所需要的密码和证书管理。

本章重点

- 数字证书
- PKI的组成
- PKI的功能
- 信任模型
- PKI相关标准

10.1　PKI概述

1976年第一个正式的公共密钥加密算法诞生，20世纪80年代初期出现了非对称密钥密码体制，即公钥基础设施(Public Key Infrastructure，PKI)。前期的PKI一直处于探索发展阶段，直到最近十年，国际上的PKI应用才开始迅速发展。

1976年，美国密码专家Diffie和Hellman提出了著名的D-H密钥体制，第一次解决了不依赖秘密信道的密钥分发问题，允许在不安全的媒体上双方交换信息，安全地获取相同的对称加密的密钥。1978年Kohnfelder提出了Certificate Agency(CA，认证机构)的概念，在CA集中式管理的模式下，公钥以CA证书的形式公布于目录库，私钥仍然以秘密信道的方式分发。1991年相继出现了PGP、PEM，第一次提出密钥由个人生成的分布式体制，以不传递私钥的方式避开了秘密信道，进一步加强了信息加密的安全性。1996年出现了SPKI解决方案，PKI设立了CA认证中心，以第三方证明的方式(即中介Agency)将公钥和标识绑定，并创立了层次化CA架构。

作为最早提出PKI的国家，美国于1996年成立了美国联邦PKI筹委会，与PKI相关的绝大部分标准都由美国制定。2000年6月30日，美国总统克林顿正式签署美国《全球及全国商业电子签名法》，给予电子签名、数字证书以法律上的保护。美国联邦政府的PKI体系建设形成了以下信任层次的信任域。

(1) 策略批准机构(PAA)：这是联邦 PKI 的根节点，负责批准二级节点的安全策略。

(2) 策略产生机构(PCA)：也叫策略认证机构，是联邦 PKI 的二级节点，定义下级产生公钥证书节点的安全策略。

(3) 认证机构(CA)：它是联邦 PKI 的三级节点，依据 PCA 定义的安全策略，为下级用户(可能是下级 CA)签发和维护数字证书、CRL 结构等。

(4) 用户：数字证书及相应私有密钥的持有者，用户利用数字证书和私有密钥进行数据维护、身份鉴别等安全行为。

除了上述层次外，联邦 PKI 体系还包含一个目录系统，用于存放有效证书和已经作废的证书。美国联邦政府在研究各联邦政府已建立的 PKI 体系的基础之上，为解决各种不同认证系统之间的交叉认证问题，于 1998 年提出了桥接 CA 的概念，旨在解决不同信任域之间的信息传输问题，避免形成信任孤岛。

加拿大在 1993 年就已经开始了政府 PKI 体系雏形的研究工作，到 2000 年已在 PKI 体系方面获得重要的进展，已建成的政府 PKI 体系为联邦政府与公众机构、商业机构等进行电子数据交换提供了信息安全的保障，推动了政府内部管理电子化的进程。

同时，欧洲在 PKI 基础建设方面的成绩也很显著。在已经颁布的 1993/1999EC 法规中，强调技术中立、隐私权保护、国内与国外相互认证以及无歧视等原则。并于 2000 年 10 月成立了欧洲桥 CA 指导委员会，于 2001 年 3 月 23 日成立了欧洲桥 CA。

在亚洲，韩国是最早开发 PKI 体系的国家。韩国的认证架构主要分三个等级：最上一层是信息通讯部，中间是由信息通讯部设立的国家 CA 中心，最下级是由信息通讯部指定的下一级授权认证机构(LCA)。日本的 PKI 应用体系按公众和私人两大领域来划分，主要分为商业、政府以及公众管理内务、电信、邮政三大块。

我国的 PKI 技术从 1998 年开始起步，政府和有关部门近年来对 PKI 产业的发展给予了高度重视，2001 年 PKI 技术被列为“十五”863 计划信息安全主题重大项目，并于同年 10 月成立了国家 863 计划信息安全基础设施研究中心。国家计委也在制订新的计划来支持 PKI 产业的发展，在国家电子政务工程中明确提出了要构建 PKI 体系。目前，全国已经推动 PKI 技术的研究与应用。2004 年 8 月 28 日，十届全国人大常委会第十一次会议表决通过了《中华人民共和国电子签名法》，规定电子签名与手写签字或者盖章具有同等的法律效力。

自从 1998 年国内第一家以实体形式运营的上海 CA 中心(SHECA)成立以来，PKI 技术在我国的商业银行、政府采购以及网上购物中得到了广泛应用。目前，国内的 CA 机构分为区域型、行业型、商业型和企业型四类；截止 2002 年底，前三种 CA 机构已经有 60 余家，58%的省市建立了区域 CA，部分部委建立了行业 CA。其中全国性的 CA 行业中心有中国金融认证中心(CPCA)、中国电信认证中心(CTCA)等。区域型 CA 有上海 CA 中心、广东电子商务认证中心等。

从 2003 年 1 月 7 日在北京召开的中国 PKI 战略发展与应用研讨会开始，我国着手组建一个国家 PKI 协调管理委员会来统管国内的 PKI 建设，由它来负责制定国家 PKI 管理政策、国家 PKI 体系发展规则，监督、指导国家电子政务 PKI 体系和国家公共 PKI 体系的建设、运行和应用。

10.1.1　理论基础

本节首先介绍一些相关的基础理论，包括基础设施和安全基础设施的概念，以及密码学的理论。

1. 基础设施概述

基础设施就是一个普适性基础，它起着基本框架的作用，例如，电子通信网络和电力供应基础设施。在电子通信网络中，局域网和广域网可以让企业内部的计算机在 Intranet 上互相交流数据，让个人用户登录 Internet 冲浪。这些设施基本原理共通，操作简便，只要遵循基本的原则，不同的实体就可以方便地使用基础设施提供的服务。

作为基础设施，需要实现"应用支撑"的功能，可以让"应用"正常工作。它应该具有以下几种特性。

- 具有易于使用、众所周知的熟悉的界面。
- 基础设施提供的服务可以预测并且有效。
- 应用设备无须了解基础设施的工作原理。

安全基础设施，同样必须依照上述的原理，同样必须提供基础服务，也就是说要具有普适性。它为整个组织提供的是保证安全的基本框架，并且可以被组织内任何需要安全的应用和对象使用。安全基础设施的"介入点"必须是统一的，便于使用的(就像墙上的电源插座一样)。

安全基础设施能够保证应用程序增强数据和资源的安全，保证增强与其他数据和资源进行交换中的安全。安全基础设施还必须具有同样友好的接入点，应用程序无须了解基础设施提供安全服务的原理，只要能够得到服务就行了。对于安全基础设施来说，能够提供一致有效的安全服务是最重要的。

2. 密码学理论

目前，密码已经从外交和军事领域走向公开，且已经发展成为一门结合数学、计算机科学、电子与通信、微电子等技术的交叉学科。使用密码技术不但可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。密码技术是信息安全技术的核心，它主要由密码编码技术和密码分析技术两个分支组成。

密码编码技术的主要任务是寻求产生安全性高的有效密码算法和协议，以满足对数据和信息进行加密和认证的要求。密码分析技术的主要任务是破译密码和伪造认证信息，实现窃取机密信息或进行诈骗破坏活动。

密码理论与技术目前主要有两大体制，即公钥密码与单钥密码(对称密码)。其中，单钥密码又可以分为分组密码和序列密码，PKI 使用的是公钥密码技术。

10.1.2　PKI 使用的密码技术

1976 年，Whitefield Diffie 和 Martin Hellman 发表了论文"New directions in cryptography"这篇文章奠定了公钥密码系统的基础。公钥密码系统的概念在密码学的发展史上具有划时代的意义。公钥密码算法又称为非对称密钥算法、双钥密码算法。

目前有两种类型的公钥系统是安全实用的，即基于大整数困难分解问题的密码体制和基于离散对数困难的密码体制。

基于大整数困难分解问题的公钥密码体制有 RSA、Rabin 体制、LUC 体制及其推广、二次剩余体制等。基于离散对数困难的密码体制主要包括基于有限域的乘法群上的离散对数问题的 ElGamal 体制和基于椭圆曲线离散对数的椭圆曲线密码体制(ECC)，以及近年来 Lenstra 等人提出的 XTR 群的离散对数问题的 XTR 公钥体制。

纠错码和密码学是两门不同的学科，但是公钥密码体制思想是建立在一个难解的数学问题之上的，即 NPC 问题。1978 年，Berlekamp 等人证明了纠错码中的一些译码问题属于 NPC 问题。这两项成果建立起纠错码和密码学相结合的理论基础。

有限自动机公钥密码体制是由我国学者陶仁骥发明的，它的思想与 RSA 体制类似。此类体制是基于分解两个有限自动机的合成而构成的，尤其是当其中的一个或两个为非线性时，难度更大。目前已经公开了该体制的三个算法，分别为 FAPKC0F、FAPKC1、FAPKC2，后者比较复杂，研究出来以支持基于身份鉴别的操作。

10.1.3　PKI 提供的安全服务

通常，一个完善的 PKI 基础设施提供的服务主要包括以下几个方面。

1. 安全登录

在访问网络资源，或者使用某些应用程序的时候，用户往往会被要求首先“登录”或者“注册”。这一步骤中，典型的操作过程包括用户输入用户身份的信息(如用户 ID 或者昵称)以及认证信息(如口令或其他机密信息)。除了合法用户没人能够获取用户的认证信息，采用这种方法能够安全地允许合法用户进入系统或者指定的应用程序。

选用一个符合安全规范的好的口令，并且记住它而不要用笔写下来，而且要经常修改口令，这对一般用户来说不是一件容易的事，很可能因为频繁更换到后来自己也不记得口令了。这正是安全基础设施提供的服务之一，它可以帮助解决这些问题。

安全基础设施并不意味着取消口令，因为口令方式是用户进入基础设施本身的认证机制。安全基础设施只是解决了使用口令方式时存在的一个最严重问题，它可以避免口令在不信任的或不安全的网络中传递，根本避免口令在传输中被截获的可能性。

使用普适性的安全基础设施可以极大地改善这种状况。安全基础设施能够将一个成功登录的结果安全地通知到其他重要登录的设备，减少远程登录的需求。

安全单点登录是安全基础设施提供的一项服务，适用于所有应用程序和设备。在任何时候和地方，如果需要使用安全传送认证信息的机制，基础设施就可以为之提供：应用程序在必要时接入基础设施，从而获得认证信息。这种基础服务减少了用户必须登录的次数。另外，在安全性上的另一个好处就是，一个设计良好的基础设施能够保证用户只需在它们工作的机器上登录。所以在某些情况下，口令无须在易于受到攻击的网络上传递，极大地降低了口令被窃听和口令存储、重复攻击的风险。

2. 终端用户透明

用户使用安全基础设施时，基础设施只是一个黑盒子，用户需要的是服务而不是如何提供服务的细节。换句话说，对终端用户而言，安全基础设施是完全透明的，这是普适性基础设施的一个极其重要的特性。

3. 全面的安全性

一个普适性安全基础设施最大的益处是在整个环境中实施的是单一的、可信的安全技术(如公钥密码技术)，所有它能够提供跟设备无关的安全服务。它能够保证数目不受限制的应用程序、设备和服务器无缝地协调工作，安全地传输、存储和检索数据，安全地进行事务处理，安全地访问服务器等。这种环境不仅极大地简化了终端用户使用各种设备和应用程序的方式，而且简化了设备和应用程序的管理工作。

使基础设施达到全面安全性所采取的重要机制之一就是保证大范围的组织实体和设备采用统一的方式使用、理解和处理密钥。为了解决 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛使用的 PKI 技术，PKI 技术采用证书管理公钥，通过第三方的可信任机构，即认证中心(Certificate Authority，CA)，把用户的公钥和用户的其他标识信息(如名称，E-mail、身份证号码等)捆绑在一起在 Internet 验证用户的身份。采用建立在 PKI 基础上的数字证书，通过对要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

10.2 数 字 证 书

公钥基础设施(Public Key Infrastructure，PKI)技术提供了网络环境下的一个安全平台，是一种具有普适性的基础设施。PKI 与非对称加密算法密切相关，同时包括消息摘要、数字签名、加解密技术等，要支持这些技术，就要用到数字证书技术。

数字证书就像身份证、护照等，是个人身份识别的凭证。形象一些来描述，它是网络上的护照。数字证书技术涉及证书签发机构(CA)、注册机构(RA)和终端用户。

由于 Internet 网络电子商务系统技术使在网上购物的顾客能够极其方便轻松地获得商家和企业的信息，同时也增加了对某些敏感或有价值的数据被滥用的风险。买方和卖方都必须对于在因特网上进行的一切金融交易运作都是真实可靠的，并且要使顾客、商家和企业等交易各方都具有绝对的信心，因此因特网电子商务系统必须保证具有十分可靠的安全保密技术，也就是说，必须保证网络安全的四大要素，即信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性。

数字证书技术是可以用来证明身份的一种技术。证书就是计算机里的一个小小的文件，类似身份证上的信息，把证件所有者的个人信息(姓名、性别、出生日期、照片等)与证件号码捆绑起来。同理，数字证书证明所有者与公开密钥的关系，也就是把证书申请者与生成的公钥绑定在一起了。

10.2.1　数字证书的定义

数字证书就是互联网通讯中标志通讯各方身份信息的数据，提供了一种在 Internet 上验证身份的方式，它由一个权威机构：CA 机构，又称为证书授权(Certificate Authority)中心发行。数字证书是一个经 CA 数字签名的包含密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。

10.2.2　数字证书的格式

目前数字证书的格式通常有 X.509 证书、WTLS 证书(WAP)、PGP 证书、属性证书等。普遍采用的是 X.509 v3 国际标准，内容包括证书序列号、证书持有者名称、证书颁发者名称、证书有效期、公钥、证书颁发者的数字签名等。

被大量接受的 X.509 国际标准格式是由 ITU-T(国际电信联盟电信标准化组织)定义的。它第一次发布在 1988 年，被推荐作为 X.500 目录系统的一部分。X.509 为 X.500 的服务提供了基于 PKI 的鉴别。1988 年发布的 X.509 的第一个版本被称为 X.509 v1 标准，可以认为是一个最早的基于 PKI 的数字证书标准的提议。1993 年修订了 X.509，增加了一些用于支持目录访问控制的内容，形成了 X.509 v2 标准。在 1993 年发布了 Internet 增强的私密电子邮件 PEM(Private Enchanced Mail)的规范 RFC1422，包括了使用基于 X.509 v1 证书的规范。ISO/IEC/ITU 和 ANSI X9 在 1996 年 6 月公布了 X.509 v3 标准。

因为 X.509 v3 是在 X.509 v2 的基础上增加了一些证书的扩展域以实现一些新的功能，所以首先介绍 X.509 v2 的证书，它的格式包括如下内容。

- Version：证书的版本号。
- Serial number：证书的序列号，这是一个由证书的发布 CA 分配的一个唯一值。
- CA 的签名算法 ID：CA 对证书签名所用的算法的标识符，支持 RSA 和 DSA。
- CA 的 X.500 名：发布证书的 CA 在 X.500 目录树上的辨识名 DN。
- 有效期：用一个起始时间和一个结束时间来表示的证书的有效周期。
- 主体名：证书所有者在 X.500 上的辨识名。
- 主体的公钥信息：包括主体的公钥、生成该密钥的算法标识符和相关信息。
- 发布者的唯一辨识符：确保证书主体的 X.500 辨识名的一个比特串，是可选域。
- 证书主体的唯一辨识符：确保证书主体的 X.500 辨识号的一个比特串，是可选域。
- Signature：签名，由 CA 私钥加密的其他字段的哈希值、签名算法标志及参数。

人们在应用中发现了 v2 的一些缺陷，无法满足设计和实施中的需要，标准的开发人员为 v3 定义了一些可选的扩展域，重要的一些扩展域内容如下。

- Certificate policies and policy mapping：证书策略和策略映射。
- Subject alternative name and issue alternative name：主体备选名和发布者备选名。
- Subject directory atrributes：主体目录属性。
- Basic constraints and name constraints：基本约束和名字约束，只出现在 CA 中。
- Authority key identifier：授权密钥标识符。
- Key usage：密钥用途。

10.2.3　数字证书的生命周期

要理解证书的生命周期，我们可以回顾一下早期的护照申请，看一下护照颁发的请求是如何进行的。

在国际上绝大多数国家中，申请护照时，用来确认申请人身份的过程通常有下述几步：①填写注册表格；②提供几个附加的证明文件；③提供几张近照；④由一名专业人士做证人；⑤遵守秩序地等候 3 小时；⑥申请时必须亲自到场；⑦必须为身份验证和证书或者护照的制作交付手续费；⑧几个星期之后正式颁发护照；⑨经过若干年，护照过期，需要重新申请。幸运的是，重新申请护照的过程相对而言比较方便和快捷，这归功于一个原因，那就是旧护照在重新申请护照时候仍然有效。因为已经有一个证明可以确定申请人的可信身份，所以仅需要重新验证一小部分资料就可以确保申请护照的人依然是旧护照持有者。

上述这个过程与申请一个数字证书需要的过程极为相似。用户与证书机构(Certificate Authority，CA)的交互是从注册机构(Registration Authority，RA)提供的用户交互界面开始的。

从证书的注册开始，需要创建公/私密钥对，并将它们关联到用于确认某个最终实体身份的证书上。作为向 CA 注册和申请证书的过程的一部分，该密钥对连同其他一些标识信息一起被提交给 CA。CA 在核实申请者身份之后，确认无误，方可颁发证书。

颁发的证书的生命期是有限的。如果到了截止日期，该证书无效，必须重新颁发一个证书。密钥有一个平均的使用寿命，在安全有效期内，证书和密钥都必须定期更新。

在某些情况下，发布最终实体证书的 CA 可能需要报废该证书。在这种情况下，该证书应该被撤销，而该 CA 需要公布这一撤销信息。

在数字证书的生命周期内，证书管理器处理应用于证书的操作集合，在完成注册过程之后，CA 必须对证书负责。证书管理包括以下过程：证书注册、证书更新、证书撤销。

1. 证书注册

与上述的申请护照的过程类似，数字证书的注册由申请人提交申请开始，并附上证书所要求的各种证明和信息，经过证书注册机构的验证校验，确认申请者的身份合法之后，方可完成注册过程。

2. 证书更新

证书在安全的有效期过期之前或者是由于某些不可预料的原因需要更新。一方面，由于安全措施上的疏忽或者软件出现的问题导致密钥泄露；另一方面，证书拥有者也许离开了颁发证书的部门单位，而之前所颁发的证书将用户与该部门单位联系在一起，所以这时候必须更新证书信息，使之前的证书和身份无效。

3. 证书撤销

大多数情况下，CA 用来公布已经更改的证书状态的机制是一个撤销证书列表。该列表包括已被撤销证书的序列号与撤销日期，还有标识撤销原因的状态。

某证书被撤销之后，通常会将这一类证书的信息存放在一个目录列表，以供证书验证时参考。证书用户在验证证书的同时也从该目录中下载了列表，并查询该列表以确认需要验证

的证书不在撤销列表之内。

证书撤销的列表有一个公布的周期，该周期时间由 CA 决定，可以是一天或者一个星期，这依赖于认证操作管理的规范定义的策略。更新该列表的频率，对于证书使用者可以寄予证书多高的信任级别有直接关系。

10.2.4　使用 Java 工具生成数字证书

与前面的密码学章节里介绍的 Java 对各种密码算法和数字签名的支持一样，JDK 1.4 加入了对 X.509 数字证书标准的支持，并将密钥库作为密钥和证书的资源库。从物理上讲，密钥库是缺省名称为.keystore 的文件。通过一个别名来区分密钥和证书，每个别名都由一个唯一的密码保护。密钥库本身也受到密码保护。Java 平台用 KeyTool 来操作密钥库，这个工具提供了许多的选项，主要有生成密钥和证书、查看密钥库、导出密钥和证书、导入证书等。同时 JDK 1.4 以上版本提供了对证书库、证书、吊销列表操作的类和方法，主要有 KeyStore 类、X509 Certificate 类、X509CRL 类，这里我们通过一个实例做一个简单介绍。

在实际应用中，常常需要获取证书相关信息，如证书版本、证书序列号、证书生效日期、证书失效日期、证书拥有者、证书颁发者、证书 DER 编码数据等。

1. 流程分析

实现以上功能的编程实现的步骤如下。

(1) 读取证书内容，创建证书对象。

```
//读取证书文件
InputStream inStream = new fileInputStream(“Justin.cer”);
//创建 X509 类
certificateFactory cf = certificateFactory.getInstance(“X.509”);
//创建证书对象
X509certificate oCert = (X509Certificate) cf.generateCertificate(inStream);
```

(2) 获取证书版本。

```
oCert.getVersion();
```

(3) 获得证书序列号。

```
oCert.getSerialNumber();
```

(4) 获取证书有效期。

```
oCert.getNotBefore();
oCert.getNotAfter();
```

(5) 获取证书主题信息、颁发者信息。

```
oCert.getSubjectDN().getName();
oCert.getIssuerDN().getName();
```

(6) 获取证书 der 编码数据。

```
Byte [] tbsCertificate = oCert.getTBSCertificate();
```

其流程图如图 10-1 所示。

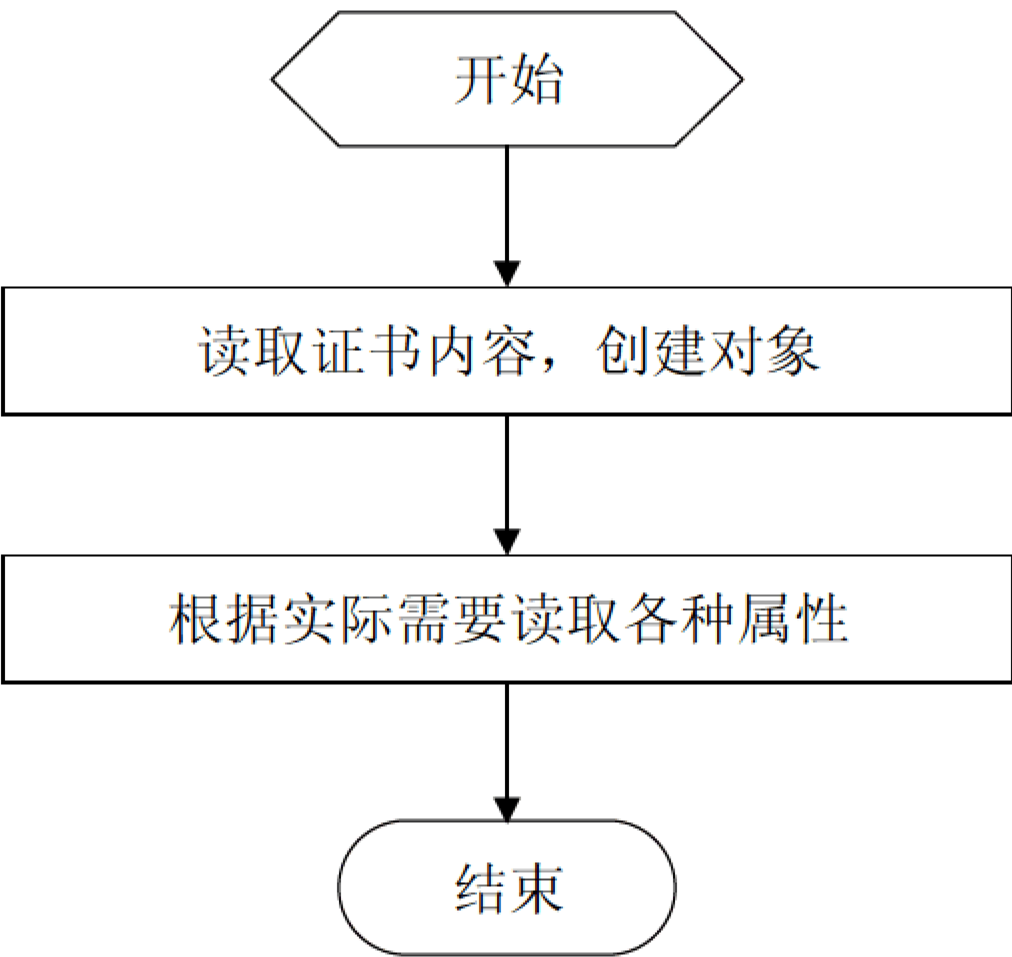


图 10-1　Java 数字证书处理流程

2. 实例实现

这里，以解析证书为例，进一步了解该系列函数的用法。程序的功能是调用 Java 安全 API 系列函数解析 Justin.cer 文件，获取相关信息。接下来以 Windows XP 平台、JDK 1.4 为例来介绍。

(1) 利用记事本或者其他编辑工具或编程工具新建文件“tCert.java”。

(2) 在 tCert.java 中，添加以下代码。

```
/*首先加载 Java 安全 API 的相关类库，从磁盘中读取证书文件 Justin.cer，然后用上一节介绍的相关函数，创建 X509 类及证书对象，从对象中获取证书版本、证书序列号、证书有效期、证书拥有者、颁发者的信息、证书签名所用的算法及证书签名值和 DER 编码数据，将这些信息打印输出。*/
//加载相关的 Java 安全 API
import java.security.*:
import javax.crypto.*:
import java.io.*:
import java.security.cert.*:
import java.text.simpleDateFormat:
import java.util.*:

public class tCert
{
    public static void main(String[] args)
    {
        //主程序调用 showCertInfo 函数
        showCertInfo();
    }
```

```
public static void showCertInfo()
{
    try{
        //读取证书文件
        InputStream inStream = new fileInputStream("Justin.cer");
        //创建 X509 类
        certificateFactory cf = certificateFactory.getInstance("X.509");
        //创建证书对象
        X509certificate oCert = (X509Certificate) cf.generateCertificate(inStream);
        inStream.close();
        SimpledateFormat dateformat = new SimpleDateFormat("yyyy/MM/dd");
        String info = null;
        //获取证书版本
        info = String.valueOf(oCert.getVersion());
        System.out.println("证书版本："+info);
        //获取证书序列号
        info oCert.getSerialNumber().toString(16);
        System.out.println("证书序列号："+info);
        //获取证书有效期
        Date beforedate = oCert.getNotBefore();
        Info = dateformat.format(beforedate);
        System.out.println("证书生效日期："+info);
        Date afterdate = oCert.getNotAfter();
        Info = dateformat.format(afterdate);
        System.out.println("证书失效日期："+info);
        //获取证书主体信息
        info = oCert.getSubjectDN().getName();
        System.out.println("证书拥有者："+info);
        //获取证书颁发者信息
        info = oCert.getIssuerDN().getName();
        System.out.println("证书颁发者："+info);
        //获取证书签名算法名称
        Info = oCert.getSigalgName();
        System.out.println("证书签名算法："+info);
        System.out.println("签名值：");
        byte[] sign = oCert.getSignature(); //获取证书签名值
        PrintHex(sign, sign.length); //打印输出证书签名值
        //获取证书 der 编码数据
        byte[] tbsCertificate = oCert.getTBSCertificate();
        System.out.println("证书 DER 编码数据：");
        PirntHex(tbsCertificate, tbsCertificate.length); //打印输出证书 DER 编码数据
    }
catch (Exception e)
{
```

```
            System.out.println("解析证书出错！");
        }
    }//end showCertInfo

    public static void PrintHex(byte data[], int lent)
    {
        int I;
        int tmp;
        String Tmp= "" ;
        for (i=0;i<len;i++) {
            if (i%16 == 0)
            {
                System.out.println("");
                //0x0000
                if(i<0x10)
                    Tmp = "0x000";
                If ((i<0x100) && (i<0x1000))
                    Tmp = "0x0";
                if(i>=0x1000)
                    Tmp = "0x";
                System.out.print(Tmp + Integer.toHexString(i)+ "h:");
            }
            tmp = data[i];
            if (tmp < 0)
                tmp = 256+tmp;
            if (tmp < 0x10)
                System.out.print("0"+Integer.toHexString(tmp)+ "");
            else
                System.out.print(Integer.toHexString(tmp) +"");
        }
        System.out.println("");
    }
}
```

10.3　PKI 的组成

PKI 是一种遵循既定标准的密钥管理平台，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。一个完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口(API)等基本构成部分。

10.3.1　概述

PKI 能够为所有网络应用，透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI 必须具有认证中心(CA)、证书库、密钥备份及恢复系统、证书废止处理系统、客户端证书处理系统等基本成分，构建 PKI 也将围绕这五大系统来进行。

10.3.2　PKI 认证机构

CA 是证书的认证机构，是 PKI 的核心。众所周知，构建密码服务系统的核心内容是如何实现密钥管理。公钥体制涉及一对密钥，即私钥和公钥，私钥只由持有者秘密掌握，无需在网上传送，而公钥是公开的，需要在网上传送。因此公钥体制的管理，主要是公钥的管理问题，目前较好的解决方案是引进证书机制。

在公钥体制环境中，必须有一个权威的、公正的、可信赖的第三方机构来对任何一个主体的公钥进行公证，证明主体的身份以及他与公钥的匹配关系。CA 正是这样的机构，它的职责归纳起来有以下几个。

- 验证并标识证书申请者的身份。
- 确保 CA 用于签名证书的非对称密钥的质量。
- 确保整个签证过程的安全性，确保签名私钥的安全性。
- 证书材料信息(包括公钥证书序列号、CA 标识等)的管理。
- 确定并检查证书的有效期限。
- 确保证书主体标识的唯一性，防止重名，发布并维护作废证书表。
- 对整个证书签发过程做日志记录。
- 向申请人发通知。

其中最为重要的是 CA 自己的密钥的管理，它必须确保其高度的机密性，防止他方伪造证书。CA 的公钥在网上公开，整个网络系统必须保证其完整性。

通常，证书应该包括以下主要内容。

(1) 证书的“用途”

规定了该证书所公证的公钥的用途，并且必须按规定的用途来使用。一般公钥又有两大类用途：一是用于验证数字签名；二是用于加密信息，进行数据加密密钥的传递。

(2) 签名密钥对

签名密钥对由签名私钥和验证公钥组成。数字签名的密钥可以有较长的生命周期。

(3) 加密密钥对

加密密钥对由加密公钥和解密私钥组成。

10.3.3　其他组成部分

为了更完善地提供安全基础服务，除了 CA 外，还需要一个存储数字证书的证书库，便于统一管理证书，进行证书的添加、删除和查询操作；为了防止意外情况发生，或者在数据破坏后进行恢复，一套完备的密钥备份以及恢复系统是必须的组成部分；证书在有效期或者到期，或者证书有效期内发生状态变更，不再需要保存相关的数据记录，则需要一套证书废

止处理系统；为了与其他的应用接口，需要一个良好的 PKI 应用接口。

1. 证书库

证书库是证书的集中存放地，它与网上的“白页”类似，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。

构造证书库的最佳方法是采用支持 LDAP(轻型目录访问协议)的目录系统，用户或相关的应用可以通过 LDAP 来访问证书库。系统必须确保证书的完整性，防止伪造、篡改证书。

2. 密钥备份及恢复系统

如果用户丢失了用于解密数据的密钥，则密文数据将无法被解密，造成数据的丢失。为了避免这种情况的出现，PKI 应该提供备份与恢复解密密钥的机制。

密钥的备份和恢复应该由可信的机构来完成，例如 CA 可以充当这一个角色。值得强调的是，密钥备份与恢复只能针对解密密钥，签名私钥不能作为备份。

3. 证书废止处理系统

证书废止处理系统是 PKI 的一个重要组件。同日常生活中的各种证件一样，证书在 CA 为其签署的有效期内也可能需要作废处理。为了实现这一个目的，PKI 必须提供作废证书的一系列机制。作废证书通常有以下的策略。

- 作废一个或多个主体的证书。
- 作废由某一对密钥签发的所有证书。
- 作废由某 CA 签发的所有证书。

作废证书一般通过将证书列入废证书表(CRL)来完成。通常，系统中由 CA 负责创建并维护一张及时更新的 CRL 表，而由用户在验证证书时负责检查该证书是否在 CRL 之列，一般是存放在目录系统中。

4. PKI 应用接口系统

PKI 的价值在于使用户能够方便地使用加密、数字签名等安全服务。因此一个完整的 PKI 必须提供良好的应用接口系统，使得各种各样的应用能够以安全、一致、可信的方式与 PKI 交互，确保所建立起来的网络环境的可信性，同时降低管理维护成本。

10.4　PKI 功能

归纳起来，PKI 应该为应用提供如下的安全支持：证书管理与 CA，密钥备份及恢复系统，交叉签证，加密密钥和签名密钥的分离，支持对数字签名的不可抵赖，密钥历史的管理，PKI 性能要求，可扩展性，互操作性，支持多应用，支持多平台。

10.4.1　证书管理

一个完善的 PKI 应该实现 CA 以及证书库、CRL 等基本的证书管理功能。

CA 是电子商务体系中的核心环节，它通过自身的注册审核体系(RA)，检查核实进行证书申请的用户身份和各项相关信息，使网上交易的用户属性客观真实，且与证书的真实性一致。认证中心作为权威的、可信赖的、公正的第三方机构，专门负责发放并管理所有参与网上交易的实体的数字证书。

RA 是数字证书注册审批机构，是 CA 的证书发放、管理的延伸。它负责证书申请人的信息录入、审核以及证书发放等工作；同时，对发放的证书完成相应的管理功能。

10.4.2　密钥管理

证书和密钥都有一定的生命周期。当用户的私钥泄露时，必须更换密钥对；其次，随着计算机速度的日益提高，密钥长度也要进行相应的调整，越来越长；另外，由于各种不可预料的因素造成的密钥或者证书的丢失、损坏，要求 PKI 具有恢复证书的功能。PKI 应该提供完全自动，无须用户干预的密钥更换以及新证书的发放服务。同时，加密和签名密钥的管理需求是相互抵触的，因此 PKI 应该支持加密和签名密钥的分离使用，避免因此造成的安全隐患。

每次更新了加密密钥之后，相应的解密密钥都应该存档，以便将来恢复用旧密钥加密的数据。每次更新签名密钥后，旧的签名私钥应该妥善销毁，防止破坏其唯一性。相应的旧验证公钥应该进行存档，以便将来用于验证旧的签名。

10.4.3　认证

数字证书认证解决了交易和结算中的安全问题，其中包括建立电子商务各主体之间的信任关系，即建立安全认证体系(CA)；选择安全标准(如 SET、SSL)；采用高强度的加密、解密技术。其中安全认证体系是关键，它决定了交易和结算是否安全进行。

CA 是整个 PKI 的关节环节，它主要负责产生、分配所有参与交易的实体所需的身份认证数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认为是安全、权威、足以信赖的机构：根认证中心(根 CA)。

认证机构为了实现其功能，一般主要由三个部分组成：注册服务器、证书申请受理和审核机构、认证中心服务器。

10.4.4　安全服务功能

具体内容如下。

1. 透明性和易用性

作为网络环境的一种基础设施，PKI 必须具有良好的性能。一般对 PKI 的性能有透明性和易用性的要求，这是对 PKI 的最基本要求。

2. 不可抵赖性

任何类型的网络安全服务都离不开这一个基本要求：不可抵赖性。

3. 可扩展性、互操作性

随着业务量的日益提升，申请注册证书和废止旧证书的数据量也相应增大，因此，证书库和废止证书列表 CRL 必须具有良好的可扩展性。

10.5 信任模型

选择信任模型(Trust Model)是构建和运作 PKI 所需的一个环节，选择正确的信任模型以及它相应的安全级别是非常重要的。同时也是部署 PKI 所要做的早期和基本的决策之一。

信任模型主要阐述了以下几个问题：一个 PKI 用户能够信任的证书是怎样被确定的；这种信任是怎样建立的；在特定环境下，这种信任如何被控制。

下面，我们简单介绍目前常见的几种信任模型：认证机构的严格层次结构模型(Strict Hierarchy of Certification Authorities Model)、分布式信任结构模型(Distributed Trust Artchitecture Model)，即网状结构模型及 Web 模型(Web Model)。

10.5.1 层次结构模型

认证机构(CA)的层次结构可以被描述为一棵倒转的树，根在顶上，树枝向下伸展，树叶在下面。在这棵倒转的树上，根代表一个对整个 PKI 系统的所有实体都有特别意义的 CA，通常叫做根 CA(Root CA)，它充当信任的根或者“信任锚”(Trust Anchor)，也就是认证的起点或终点。在根 CA 的下面是零星的或多层中介 CA(Intermediate CA)，也被称为子 CA(Subordinate CA)，因为它们从属于根 CA。子 CA 用中间节点表示，从中间节点再伸出分支。与非 CA 的 PKI 实体相对应的树叶通常被称为终端实体(End Entities)或称为终端用户(End Users)。在这个模型中，层次结构中的所有实体都是信任唯一的根 CA。这个层次结构按如下规则建立。

根 CA 认证(准确地说是创立和签署证书)直接连接在它下面的 CA。每个 CA 都认证零个或多个直接连接在它下面的 CA。倒数第二层的 CA 认证终端实体。

在认证机构的层次结构中，每个实体(包括中介 CA 和终端实体)都必须有根 CA 的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础。因此，它必须通过一种安全的方式来完成。

10.5.2 分布式网状结构模型

与在 PKI 系统中的所有实体都信任唯一的一个 CA 的严格层次结构相反，分布式信任结构把信任分散在两个或多个 CA 上，形成一个网状的结构。也就是说，A 把 CA1 作为它的信任锚，而 B 可以把 CA2 作为它的信任锚。因为这些 CA 都作为信任锚，因此相应的 CA 必须是整个 PKI 系统的一个子集所构成的严格层次结构的根 CA(CA1 是包括 A 在内的层次结构的根，CA2 是包括 B 在内的层次结构的根)。

如果这些层次结构都是可信颁发者层次结构，那么该总体结构就被称为完全同位体结构

(Fully Peered Architecture)，因为所有的 CA 实际上都是相互独立的同位体(在这个结构中没有 CA)。另一方面，如果所有的层次结构都是多层结构(Multi Level Hierarchy)，那么最终的结构就被叫做满树结构(Fully Treed Architecture)。

混合结构(Hybrid Treed Architecture)也是可能的(具有若干个可信颁发者层次结构和若干个多层树型结构)。一般来说，完全同位体结构部署在某个组织内部，而满树结构和混合结构则是在原来相互独立的 PKI 系统之间进行互联的结果。尽管“PKI 网络(PKI Networking)”一词用得越来越多(特别对满树结构和混合结构)，但是同位体根 CA(Peer Root CA)的互连过程通常被称为“交叉认证(Cross Certification)”。

10.5.3　Web 模型

Web 模型是在 WWW 上诞生的，并且依赖于流行的浏览器，如以前的 Netscape 公司的 Navigator 和 Microsoft 公司的 Internet Explorer。在这种模型中，许多 CA 的公钥被预装在标准的浏览器上。这些公钥确定了一组浏览器用户最初信任的 CA，尽管这组根密钥可以被用户修改，然而几乎没有普通用户对于 PKI 和安全问题能精通到可以进行这种修改。

初看之下，这种模型似乎与分布式信任结构模型相似，但从根本上讲，它更类似于认证机构的严格层次结构模型。因为在实际上，浏览器厂商起到了根 CA 的作用，而与被嵌入的密钥相对应的 CA 就是它所认证的 CA，当然这种认证并不是通过颁发证书实现的，而只是物理地把 CA 的密钥嵌入浏览器。

Web 模型在方便性和简单互操作性方面有明显的优势，但是也存在许多安全隐患。例如，因为浏览器的用户自动地信任预安装的所有公钥，所以即使这些根 CA 中有一个是“坏的”，例如，该 CA 从没有认真核实被认证的实体，安全性将被完全破坏。A 将相信任何声称是 B 的证书都是 B 的合法证书，即使它实际上只是由公钥嵌入浏览器中的坏的 CA 签署的挂在 B 名下的 C 的公钥。所以，A 就可能无意间向 C 透露机密或接受 C 伪造的数字签名。

当然，在其他信任模型中也可能出现类似的情况。例如在分布式信任模型中，A 或许不能认可一个特定的 CA，但是在其软件在相关的交叉认证是有效的情况下，却会信任该 CA 所签署的证书。在分布式信任结构中，A 在 PKI 安全方面明确地相信其局部 CA“做正确的事”，例如，与可信的其他 CA 进行交叉认证等。而在 Web 模型中，A 通常因为与安全无关的原因而取得浏览器的信任，因此，从这个安全观点来看，没有任何理由相信这个浏览器是在信任“正确的”CA。

另一个潜在的安全隐患是没有实用的机制来撤销嵌入到浏览器中的根密钥。如果发现一个根密钥是“坏的”(就像前面所讨论的那样)或者与根的公钥相对应的私钥被泄密了，要使全世界数百万个浏览器都自动地废止该密钥的使用，是不可能的。这是因为无法保证通报的报文能到达所有的浏览器，而且即使报文到达了浏览器，浏览器也没有处理该报文的功能。因此，从浏览器中去除坏密钥，需要全世界的每个用户都同时采取明确的动作，否则，一些用户将是安全的而其他用户仍处于危险中，但是这样一个全世界范围内的同时动作是不可能实现的。

最后，该模型还缺少有效的方法在 CA 和用户之间建立合法的协议，该协议的目的是使

CA 和用户共同承担责任。因为浏览器可以自由地从不同站点下载，也可以预装在操作系统中，CA 不知道(也无法确定)它的用户是谁，并且一般用户对 PKI 也缺乏足够的了解，因此不会主动与 CA 直接接触。这样，所有的责任最终或许都会由用户来承担。

10.6　相关的标准

两个 PKI 应用程序之间要进行交互，只有互相理解对方发来的数据的字节的含义才可能实现。标准提供了数据语法和语义的共同约定。最常见的PKI 应用程序格式标准是 X.509 标准，因为它定义了公钥证书的基本结构。RSA 实验室的 PKCS 标准是定义数据比特含义的主要标准。这些标准定义了如何恰当地格式化私钥或者公钥。其他重要的标准包括 PKIX 证书和 CRL 概要文件、X.500 目录服务协议和 LDAP 轻型目录访问协议。

10.6.1　X.509 标准

X.509 是国际电信联盟——电信(ITU-T)部分标准和国际标准化组织(ISO)的证书格式标准。作为 ITU-ISO 目录服务系列标准的一部分，X.509 定义了公钥证书的基本标准。1988 年首次发布，1993 年和 1996 年两次修订，当前版本是 X.509v3，它加入了扩展字段的支持，极大地增进了证书的灵活性。X.509v3 证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段。即使在强制字段中，X.509 证书也允许很大的灵活性，因为它为大多数字段提供了多种编码方案。

10.6.2　PKIX 标准

IETF 的安全领域的公钥基础设施(PKIX)工作组正在为互联网上使用的公钥证书定义一系列的标准。PKIX 工作组在 1995 年 10 月组成，目的是要开发必须的互联网标准来支持可互操作的 PKI。工作组的第一项任务是要创建一个概要文件，把证书数据结构、扩展域和数据取值限定在一个特定的可选范围内。X.509 标准的巨大灵活性使得互操作难以实现；PKIX 工作组希望通过限制允许的选项，提高 PKI 系统间的互操作性。

PKIX 工作组定义了公钥证书及 CRL 的概要文件。在一些情况下，它还定义了其他的证书扩展字段或证书属性，还有这些属性的对象标识。PKIX 也正在开发新的协议以便于 PKI 生命周期中自始至终对 PKI 信息的管理。这些协议大部分都在本章讨论，包括证书管理协议(CMP)、安全多用途邮件扩展(S/MIME)和在线证书状态协议(OCSP)等。

10.6.3　PKCS 标准

公钥密码标准(PKCS)是由 RSA 实验室与工业界、学术界和政府代表合作，最初为了推进公钥密码系统的互操作性而开发的。在 RSA 带领下，PKCS 的研究随着时间不断发展，涉及了不断发展的 PKI 格式标准、算法和应用程序接口。PKCS 标准提供了基本的数据格式定义和算法定义，它们实际上是今天所有 PKI 实现的基础。

PKCS 标准包括如下内容。

- PKCS #1 RSA 加密标准。
- PKCS #2 RSA 的消息摘要加密。
- PKCS #3 Diffie-Hellman 密钥协议标准。
- PKCS #4 最初是规定 RSA 密钥语法。
- PKCS #5 基于口令的加密标准。
- PKCS #6 扩展证书语法标准。
- PKCS #7 密码消息语法标准。
- PKCS #8 私钥信息语法标准。
- PKCS #9 可选属性类型。
- PKCS #10 证书请求语法标准。
- PKCS #11 密码令牌接口标准。
- PKCS #12 个人信息交换语法标准。
- PKCS #13 椭圆曲线密码标准。
- PKCS #14 伪随机数产生标准。
- PKCS #15 密码令牌信息语法标准。

10.6.4　X.500 标准

X.500 是一套已经被国际标准化组织(ISO)接受的目录服务系统标准，由国际电报电信咨询委员会(Consultative Committee of International Telegraph and Telephone，CCITT)在 1988 年制定第一版，1993 年国际电信联盟电信标准化部门(简称 ITU-T，由 CCITT 改组而成)做了显著的修订和补充，产生了第二版。它定义了一个机构如何在全局范围内共享其名字和与之相关的对象，是一组标准的集合，定义了分布式目录服务，是一套完整的信息存储机制，包括信息模型、认证框架、命名空间、功能模型、分布式操作模型以及复制机制、搜索机制和用于客户机/服务器的通信访问协议等。X.500 系列标准由以下 9 个标准组成。

- X.500 目录服务的概要介绍。
- X.501 定义了目录服务的模型。
- X.511 对目录的各个抽象服务做了定义。
- X.518 描述分布操作的实现过程。
- X.519 是传输协议。
- X.520 和 X.521 定义了常用对象类和属性。
- X.509 提出了一种认证的框架。
- X.525 描述了复制机制。
- X.530 描述了在 OSI 七层协议模型上的 X.500 目录服务管理。

X.500 系列标准的目录服务是分布式的，每个目录的用户由一个目录用户代理(Directory User Agent，DUA)代表，它就是用户用于访问目录服务的进程。在用户看来，这个目录在逻辑上是统一的整体，但实际上目录信息可能分布在不同组织管理的计算机上，这些计算机中运行的相互配合提供服务的进程是目录服务代理(Directory Server Agent，DSA)。

X.500 目录服务可以提供域内的用户和资源信息。在 X.500 目录结构中，通过目录访问协议 (Directory Access Protocol，DAP)，客户机查询并接收来自服务器目录服务器中上的响应，从而实现对服务器和客户机之间的通信控制。

X.500 主要具备以下特征。

- 分散维护(Decentralized Maintenance)：运行于 X.500 的每个站点只负责本地目录部分，所以可以立即进行更新和维护操作。
- 强大的搜索性能：X.500 具有强大的搜索功能，支持用户建立的任意复杂查询。
- 单一全局命名空间(Single Global Namespace)：类似于 DNS，X.500 可为用户提供单一同性命名空间(Single Homogeneous Namespace)。与 DNS 相比，X.500 的命名空间更加灵活且易于扩展。
- 结构化信息结构(Structured Information Framework)：X.500 目录中定义了信息结构，允许本地扩展。
- 基于标准的目录服务(Standards-Based Directory Services)：X.500 可以被用于建立一个基于标准的目录，发送请求的应用程序能访问这些目录信息。

X.500 是层次性的，其中的管理域(机构、分支、部门和工作组)可以提供这些域内的用户和资源信息。在 PKI 体系中，X.500 被用来唯一标识一个实体，该实体可以是机构、组织、个人或一台服务器。X.500 被认为是实现目录服务的最佳途径，其优势是具有信息模型、多功能和开放性。但是 X.500 需要较大的投资，并且比其他方式速度慢。

由于 X.500 严格遵照 OSI 七层协议模型，充分利用了 OSI 协议的表示层服务。要求系统安装庞大的 OSI 协议栈，而普通 PC 无法安装，并且在 Internet 上最广泛使用的 TCP/IP 协议体系不包括表示层，限制了 X.500 在 Internet 上的应用。为了解决这个问题，密歇根州大学推出了一种较为简单的基于 TCP/IP 的 DAP 新版本，即轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)，主要用在 Internet 上，LDAP 与 DAP 具有很多类似的基本功能，另外它还能用来查询权限目录或开放 X.500 服务上的数据。

10.6.5　LDAP 标准

轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)是在 X.500 标准基础上产生的一个简化版本，是X.500标准中目录访问协议(DAP)的一个子集，简化了完整的X.500实现功能，并扩展了对 TCP/IP 协议体系的支持，这是与 X.500 最大的不同之处，是访问 Internet 必须的。用户只要安装了 TCP/IP 协议就能够访问 X.500 目录，LDAP 也可以用于建立 X.500 目录。

LDAP 协议于 1993 年获批准，产生 LDAP v1 版。之后由于考虑到 RSA 的复杂性，出现了第二代的 LDAP，即 LDAP v2，它可以提供独立的目录服务，采用了简单的编码方式，并且在 TCP/IP 上实现。但是 LDAP v2 没有提供访问控制，访问安全方面仅在绑定目录时提供了明文密码和 Kerberos 两种选项。1997 年发布新的 LDAP v3 版，该版本是 LDAP 协议发展的一个里程碑，提供了很多自有的特性，使 LDAP 功能更加完善，具有很大的生命力。

1. LDAP 与 X.500 的区别

LDAP 与 X.500 的区别与联系如下。

- LDAP 是基于 X.500 的一个 X.500 的访问机制。
- LDAP 是 X.500 简化的目录访问方法和目录结构。
- LDAP 通信是基于 TCP/IP 的，而 X.500 标准中的 DAP 采用 OSI 协议技术栈支持。
- LDAP 必须根据 X.500 来提供服务，但并不是在提供服务的过程中使用协议。

2. LDAP 的组成

LDAP 是一系列协议组成的，主要包括以下内容。

- RFC 2251：LDAPv3 核心协议，定义了 LDAP v3 协议的基本模型和基本操作。
- RFC 2252：定义 LDAP v3 基本数据模式(Schema)。
- RFC 2253：定义 LDAP v3 中的分辨名(DN)表达式。
- RFC 2254：定义 LDAP v3 中的过滤表达式。
- RFC 2255：定义 LDAP v3 统一资源地址的格式。
- RFC 2256：定义 LDAP v3 使用 X.500 的 Schema 的列表。
- RFC 2829：定义 LDAP v3 中的认证方式。
- RFC 2830：定义了如何通过扩展使用 TLS 服务。
- RFC 1823：定义了 C 的 LDAP 客户端 API 开发接口。
- RFC 2847：定义了 LDAP 数据导入、导出文件接口 LDIF。

3. LDAP 的特点

(1) 层次结构清晰，数据存取速度快

LDAP 是专门为数据的查询服务优化的，基于树状的层次结构大幅度缩短了检索所需要的时间。对于数据的修改，LDAP 假定修改操作远小于查询操作所占的比例。

(2) 同步复制和分布式服务功能

大部分 LDAP Server 都提供了自动复制备份功能，保证了数据的安全和同步，并且通过索引功能支持分布式的 LDAP 服务。

(3) 可以跨平台和系统

LDAP 协议位于 TCP/IP 的上层，与具体的操作系统无关，服务器提供的是标准统一的接口，各种平台的服务器端可以通过 LDAP 端口进行数据存取。

(4) 完善的安全控制设施

LDAP 服务可以使用标准的 SSL 连接(LDAPS)，保证连接的机密性，并且对于自身数据的访问也允许通过 ACL(访问控制列表)控制，严密的安全措施保证了数据的可靠性，内置的 ACL 可以根据访问者身份，访问数据的信息，数据存放的位置以及其他相关信息对数据进行访问控制，LDAP 目录服务器负责这些访问权限的控制，因此客户端的应用程序就可以避免与自身控制无关的安全检查。

同时，由于 LDAP 协议的开放性和众多的 LDAP 服务器端和客户端免费应用软件的开发使用，LDAP 越来越受到业界的广泛认同。LDAP 的广泛应用与流行又进一步促进了 LDAP 自身的不断发展，而各个软件厂商也在各自的产品中加入了对 LDAP 的支持。因此在公共信息查询与存储领域，LDAP 具有广泛的影响力。

本 章 小 结

本章从 PKI 基础知识出发，描述了 PKI 系统部件、组成以及各种相关协议标准，从技术层面介绍了 PKI 的实现技术和系统架构，希望通过本章的学习能够对用户了解、研发、建设和应用 PKI 起到帮助，掌握基础的网络安全协议知识，为后面章节的学习打下坚实的基础。

课 后 练 习

一、填空题

1. 从密钥密码体制的分类来看，PKI 属于(　　　　　)体制。
2. 数字证书是网络上的(　　　　　)，它的技术涉及三方面机构，分别是(　　　　　)、(　　　　　)、(　　　　　)。
3. JDK 1.4 以上版本提供了对数字证书的应用程序接口类，主要有(　　　　　)、(　　　　　)、(　　　　　)。
4. 本章介绍了几种常见的信任模式，分别是(　　　　　)、(　　　　　)、(　　　　　)。
5. 本章介绍的几种标准中，(　　　　　)是实际上所有 PKI 实现的基础。

二、选择题

1. 下列特性中，属于 PKI 的特性的是(　　)。
   A. 易于使用　　B. 可以预测　　C. 透明性　　D. 不可抵赖性
2. PKI 基础设施提供的安全服务，包括下面的(　　)。
   A. 安全登录　　B. 可以预测　　C. 透明性　　D. 不可抵赖性
3. 下述选项中，(　　)是 PKI 事实上的行业标准。
   A. X.509　　B. PKCS　　C. X.500　　D. LDAP
4. 下述特点中，属于 LDAP 具备的特点有(　　)。
   A. 层次结构　　B. 分布式服务　　C. 跨平台　　D. 速度快
5. X.500 所包含的标准，包括以下的(　　)。
   A. X.501　　B. X.511　　C. X.509　　D. X.525

三、 简答题

1. PKI 具有什么样的特性？
2. 描述数字证书的生命周期经历哪几个阶段。
3. 简单说明 LDAP 与 X.500 的区别。
4. 简述 PKCS 的标准内容。
5. 简述 X.500 标准包含几个标准及其内容。

第11章　网络安全技术

随着 Internet 的发展和网上电子商务的繁荣，Internet 已从最初仅用于军方及科研机构的网络转变成了一个庞大的商业通信骨干网。越来越多的企业、部门和组织加入进来，新的应用领域不断扩展，很多企业都希望在 Internet 上开展自己的业务，而个人也希望 Internet 能提供更多的服务。人们对 Internet 的依赖性越来越强，同时也意味着 Internet 的安全性正成为人们关注的焦点。

本章重点

- 链路加密与端到端加密的概念及特点
- 按过滤原理划分防火墙类型及其特点
- 入侵检测系统部署方法
- VPN 的主要应用场合、特点

11.1　网络数据加密技术

网络数据加密技术是网络安全保障的最基本要求。密码学作为网络安全的核心，得到了广泛的应用。理论上，加密操作可以在 OSI 模型中的任意层上进行。但在实际应用中，加密机制一般放在较低层，这样能以较小的开销获得较好的安全效果。加密方式通常分为两种：链路加密、端到端加密。

11.1.1　链路加密

链路加密可用于任何类型的数据通信链路。因为链路加密要对通过这条链路的所有数据进行加密，通常在物理层或数据链路层实施加密机制。链路加密方式如图 11-1 所示。

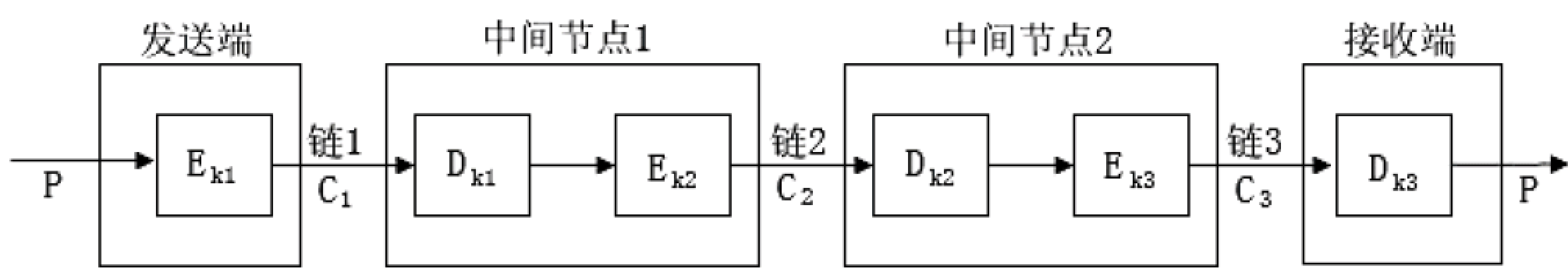


图 11-1　链路加密工作原理

由图 11-1 可知，链路加密的工作原理是，数据报 P(明文)经发送端的加密设备处理后(加密动作为 E，使用密钥 K1)变成 C_1(密文)，发送到链路 1 上传输，到达中间节点 1。在中间节

点 1 内，首先由解密设备将 C1 进行解密操作(解密动作为 D，密钥使用 K1)，恢复为 P，再进行相关处理。在发送到链路 2 之前，再由加密设备对 P 进行加密(使用密钥 K2)。在中间节点 2 和接收端也采取类似的处理过程。

链路加密的优点在于，对用户透明，能提供流量保密性，密钥管理简单，提供主机鉴别，加密和解密都是在线进行的。缺点是：数据仅在传输线路上是加密的，在发送主机和中间节点上都是暴露的明文形式，容易受到攻击。此外，网络中的每条物理链路都必须加密，当网络很大时，加密和维护的开销大，而且每段链路需要使用不同的密钥。因此，在使用链路加密时，必须保护主机和中间节点的安全。

11.1.2　端到端加密

端到端加密是指数据在发送端被加密后，通过网络传输，到达接收端后才被解密。端到端加密方式如图 11-2 所示。

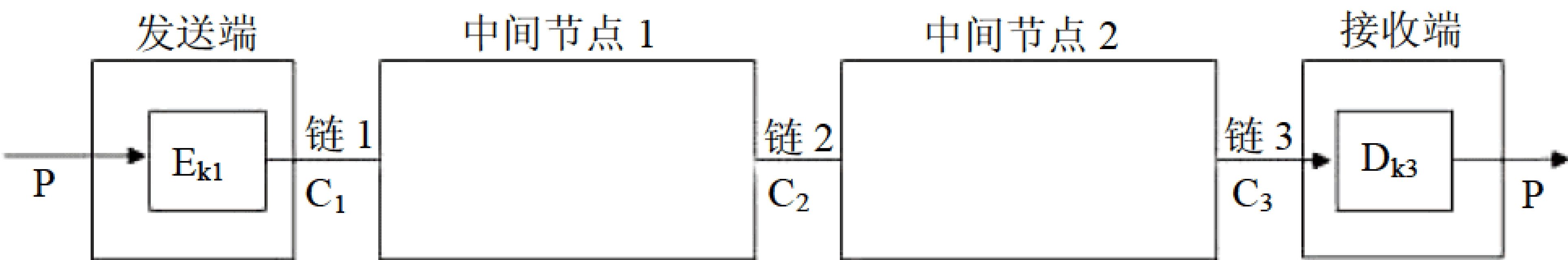


图 11-2　端到端加密工作原理

在端到端加密方式中，数据在发送端被加密后，一直保持加密状态在网络中传输。这样做有两个好处，一是避免了每段链路的加密解密开销，二是不用担心数据在中间节点被暴露。

在端到端加密方式中，加密机制可放置在不同的位置，如应用层、网络层或数据链路层。端到端加密方式通常采用软件来实现。端到端加密方式的主要优点是，在发送端和中间节点上数据都是加密的，安全性好。这种方式提供了更灵活的保护手段，能针对用户和应用实现加密，用户可以有选择地应用加密，并能提供用户鉴别。主要缺点是：不能提供流量保密性，需要用户来选择加密方法和决定算法，每对用户需要一组密钥，密钥管理系统复杂。这种方式只有在需要时才进行加密，即加密是离线的。

11.2　防　火　墙

传统意义上的防火墙(Firewall)是指建筑间实现区域隔离、阻止火势蔓延的设施，如图 11-3 所示。

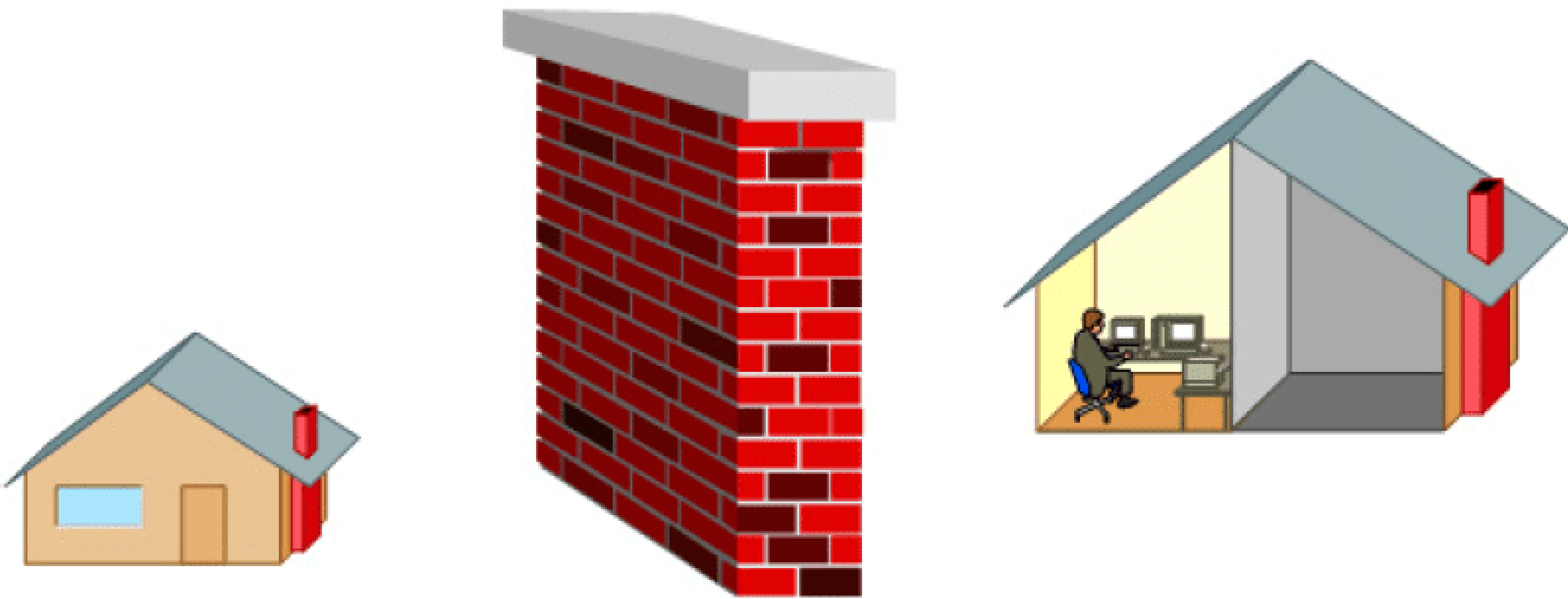


图 11-3　传统意义上的防火墙

网络防火墙是在两个不同网络安全区域之间执行访问控制策略的一个或一组系统，包括硬件和软件。防火墙遵循的是一种允许或阻止业务来往的网络通信安全机制，提供可控的过滤网络通信，只允许授权的通信，目的是保护网络不被他人侵扰。

11.2.1　防火墙概述

通常，防火墙就是位于内部网络或 Web 站点与 Internet 之间的一个路由器或一台计算机，又称堡垒主机，它是对所有网络通信流进行过滤的节点，是两个或多个安全域之间通信流的唯一通道，如图 11-4 所示。

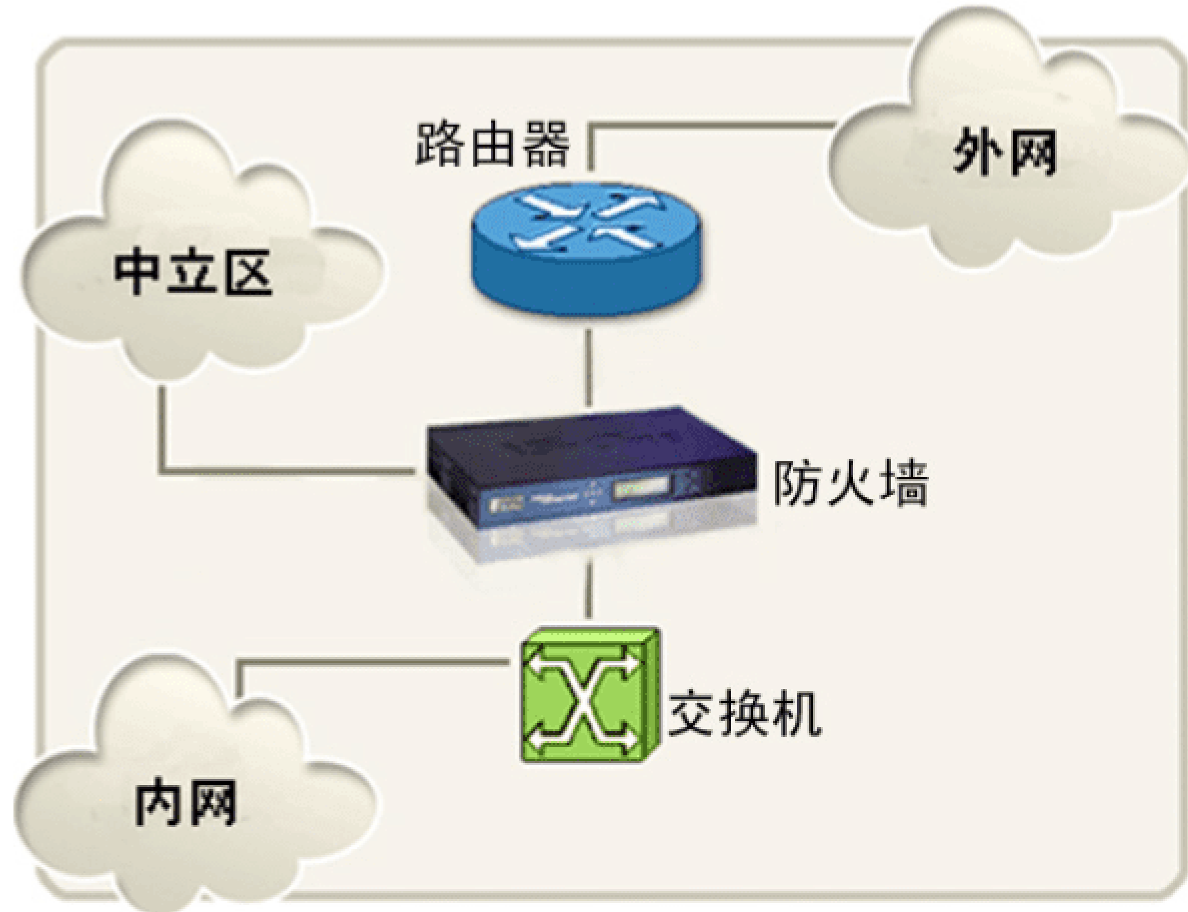


图 11-4　传统意义上的防火墙

防火墙通过审查经过堡垒主机的每一个数据包，判断它是否匹配事先设置的过滤规则(又称访问控制列表(Access Control List，ACL)。如满足，根据控制机制做出相应的动作，不满足则将数据包丢弃，以保护网络的安全。

防火墙根据 ACL 对数据包进行匹配操作时，有两种基本策略。第一种，除非规则指明的数据包允许通过，其余数据包均被禁止通过，这种规则被称为限制策略。第二种，除非规则指明的数据包禁止通过，其余数据包均允许通过，这种规则被称为宽松策略。为了提高安全性，通常防火墙均采用限制策略，但限制策略配置过程相对复杂一些。

11.2.2　防火墙的功能及其局限性

通过在网络中部署防火墙，可以实现以下功能。

1. 隐藏内部网络

防火墙为用户的内部网络创建了一个可保护的边界，并且隐藏了内部网络的一些信息以增加保密性。当入侵者从外部测试用户的内部网络时，只能看到防火墙，而内部网络的拓扑、布局等信息都将被屏蔽。防火墙通过提高认证功能和对网络加密来限制网络信息在向外部传输过程中暴露，并可限制从外部发起的攻击。

2. 控制内部网络对外部网络的访问

该功能分为两方面：一方面是可以控制内网用户对外部一些非法或者受限网络的访问，另一方面是控制内网用户是否可以连接到外部网络。前者是通过对外部 IP 或者网址的控制来

实现的，后者是通过对内部用户的 IP 控制来实现的。

3. 控制外部网络用户对内部网络的访问

该功能也分为两方面：一方面是只允许外部用户访问本地网络中的某些主机，另一方面是只允许外部用户中指定的用户访问本地网络。前者是通过控制本地 IP 来实现的，后者通过控制外部 IP 来实现。

4. 监视网络安全，提供安全日志并预警

这是防火墙最主要的作用之一，根据防火墙提供的日志，可以判断是否有异常的连接请求，对于可疑的网络操作，如多次连续的失败请求等，则需注意是否是入侵者开始的试探性攻击。

5. 缓解 IP 地址空间紧张问题

内部网络在连接到 Internet 时，可能会获得比较少的几个外部网络 IP 地址(又称公网 IP)，可以通过防火墙的网络地址转换(Network Address Translation，NAT)功能，将有限的 IP 地址动态或静态与内部的 IP 地址对应起来，这种办法可以缓解地址空间不足的问题。

6. 对内部用户的 Internet 访问进行审计和记录

防火墙是审计和记录 Internet 使用情况的一个最佳地点。管理员可以在此对 Internet 的使用情况进行了解，查出潜在的带宽瓶颈位置，并及时对 Internet 的使用情况进行调整。

7. 引出 DMZ(Demilitarizde Zone，非军事区，又称中立区)

从防火墙可以连接到一个单独的网段上，即 DMZ 区，并在此部署 WWW 服务器和 FTP 等服务器，将其作为向外部发布内部信息的地点。

除了上面的功能外，某些防火墙还具备一些流量控制和抵御 DoS 攻击的功能。

选择网络安全设备时，配备并正确配置防火墙，是保障网络安全的基本要求。但并非有了防火墙就可以高枕无忧。传统防火墙存在以下诸多局限性。

- 防火墙不能防范不经过防火墙的攻击，也就是说，不经过防火墙的数据，防火墙无法检查、防护。
- 防火墙不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内，内外都不可信，但很多时候，因为实施难度以及用户使用方便性等问题，将防火墙配置为只防护外网的方式。
- 防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全，而不能自作主张。
- 防火墙不能防止可接触的(即物理的)人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。
- 防火墙不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议，防火墙不能防止利用该协议中的缺陷进行的攻击。

- 防火墙不能防止利用服务器系统漏洞进行的攻击。攻击者通过防火墙允许的访问端口对该服务器的漏洞进行攻击，防火墙无法阻止。
- 防火墙不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。
- 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或拷贝到内部网的主机上并执行时，可能会发生数据驱动式的攻击，防火墙无法过滤这类数据。
- 防火墙不能防止内部的泄密行为。如防火墙所保护的内网用户主动泄密，防火墙就无能为力。
- 防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞，因此对防火墙也必须提供某种安全保护。

11.2.3　防火墙的分类

按不同的分类方法，防火墙可分为多种不同类型。

1. 按存在形式划分

按存在形式的不同，防火墙可以分为软件防火墙、硬件防火墙及芯片级防火墙。

(1) 软件防火墙

软件防火墙运行于特定的计算机上，它需要客户预先安装好计算机操作系统，一般来说这台计算机就是整个网络的网关。软件防火墙就像其他的软件产品一样需要先在计算机上安装并做好配置才可以使用。防火墙厂商中做网络版软件防火墙最出名的莫过于以色列的 Checkpoint。使用这类防火墙，需要网管对所工作的操作系统平台比较熟悉。

(2) 硬件防火墙

这里说的硬件防火墙是指所谓的“硬件防火墙”。之所以加上“所谓”二字是针对芯片级防火墙而言的，它们的最大差别在于是否基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙，它们都基于 PC 架构，就是说，它们和普通的家庭用的 PC 没有太大区别。在这些 PC 架构计算机上运行一些经过裁剪和简化的操作系统，最常用的是 Unix、Linux 和 FreeBSD 系统。值得注意的是，由于此类防火墙采用的依然是别人的内核，因此依然会受到 OS(操作系统)本身的安全性影响。

传统硬件防火墙一般至少应具备三个端口，分别接内网、外网和 DMZ，当前新的硬件防火墙往往扩展了端口，常见四端口防火墙一般将第四个端口作为配置口、管理端口。很多防火墙还可以进一步扩展端口数量。

(3) 芯片级防火墙

芯片级防火墙基于专用的硬件平台及专用的操作系统。专用的 ASIC 芯片促使它们比其他的防火墙速度更快，处理能力更强，性能更高。这类防火墙的知名厂商有 NetScreen、FortiNet、Cisco 等。这类防火墙由于是专用操作系统，因此本身的漏洞比较少，但价格相对比较高昂。

2. 按过滤原理划分

按对数据包的过滤原理划分，防火墙可以分为“包过滤型”和“应用代理型”两大类。前者以 Checkpoint 防火墙和美国 Cisco 公司的 PIX 防火墙为代表，后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

(1) 包过滤(Packet Filtering)防火墙

包过滤型防火墙工作在网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许数据包通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。通用是指因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务。廉价是指大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的。有效是指它能很大程度上满足绝大多数企业的安全要求。

在防火墙技术发展过程中，包过滤技术出现了两种不同版本，称为第一代静态包过滤和第二代动态包过滤。

第一代静态包过滤防火墙几乎与路由器同时产生，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括源 IP 地址、目标 IP 地址、源端口号、目的端口号等。

静态包过滤防火墙配置 ACL 的格式为：

```
permit/deny   sourceip   sourceport   destip   destport   direction
```

permit 表示允许(某动作)，deny 表示禁止(某动作)。

direction 表示方向，值为“in”表示进入(从外网到内网)，“out”表示出去(从内网到外网)。

利用此类防火墙，内网用户可以访问外网的 Web 服务，典型的配置过程如下，这里假定都使用 TCP 协议。

首先，需要配置一条 ACL，使得内网用户可以发起向外网的连接，如图 11-5 所示。

动作	源地址	源端口	目标地址	目标端口	方向
允许	*	*	*	80	出

图 11-5　允许内网发起向外网的 80 端口 TCP 连接的 ACL

这条 ACL 中，源 IP 为*(有的设备用 0.0.0.0 表示)，表示允许所有内网用户访问外网的 Web 服务。因向外发起 TCP 连接时，源端口又是不固定的，由操作系统临时分配一个范围为 1024~65535 的值，因而这条 ACL 中源端口为*(有的设备用 0 表示)，表示允许所有源端口发起向外网的 Web 服务(TCP 80 端口)的连接，同样，这里的目的 IP 也为*。方向“出”表示是由内向外的连接。在对防火墙进行配置时，这条 ACL 的写法如下。

```
permit   0.0.0.0   0   0.0.0.0   80   out
```

然后，需要配置一条 ACL，使得外网 Web 服务器可以向内网用户发起 Web 请求连接对

应的确认连接，如图 11-6 中深色部分所示。需要注意的是，因为内网用户发起连接时的端口是不确定的，范围为 1024~65535，因而第二条 ACL 中，向内网用户发起的确认连接中，目的端口也必须为 1024~65535。

动作	源地址	源端口	目标地址	目标端口	方向
允许	*	*	*	80	出
允许	*	80	*	1024-65535	进

图 11-6　允许外网发起向内网确认连接的 ACL

第二条 ACL 的写法是：

```
permit    0.0.0.0    80    0.0.0.0    1024-65535    in
```

有了这两条 ACL，即可实现内网用户访问外网的 Web 服务，且外网 Web 服务器可以向内网用户发起确认连接。然而，观看这两条 ACL 可以发现，其中第二条会导致内网用户大范围的端口(1024~65535)都被防火墙打开，这显然是非常不安全的做法。这是第一代静态包过滤防火墙的致命缺陷，事实上，目前已不存在作为单纯的防火墙产品出现的静态包过滤防火墙，而均被动态包过滤防火墙所取代。

第二代动态包过滤防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为状态检测(Stateful Inspection)技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，建立相应的状态表，并依据状态表动态地在过滤规则中增加或更新条目。当前成熟的动态包过滤防火墙均为状态检测防火墙，其中，Checkpoint 的产品是典型的成功案例。

考虑同样的问题，要求允许内网用户访问外网的 Web，在状态检测防火墙中，只需设置一条与图 11-5 相同的 ACL 即可，无需开放其内网用户的大量端口。其基本工作原理是，当内网用户向外网 Web 服务器发起连接时，根据图 11-5 的 ACL，连接被允许，此时，会在防火墙内建立一个状态表，以描述该内网用户与外网 Web 服务器的连接状态。当外网 Web 服务器向该内网用户发起 Web 服务请求的确认连接时，根据状态表的内容，该请求将被允许操作，而无需匹配其他 ACL。简言之，状态检测防火墙在判断数据包是否允许通过时，依据的不仅仅是 ACL 还有状态表，或者说状态检测防火墙对数据包进行判断时，在 ACL 的基础上，还要查看各个数据包之间的联系，如图 11-7 所示。

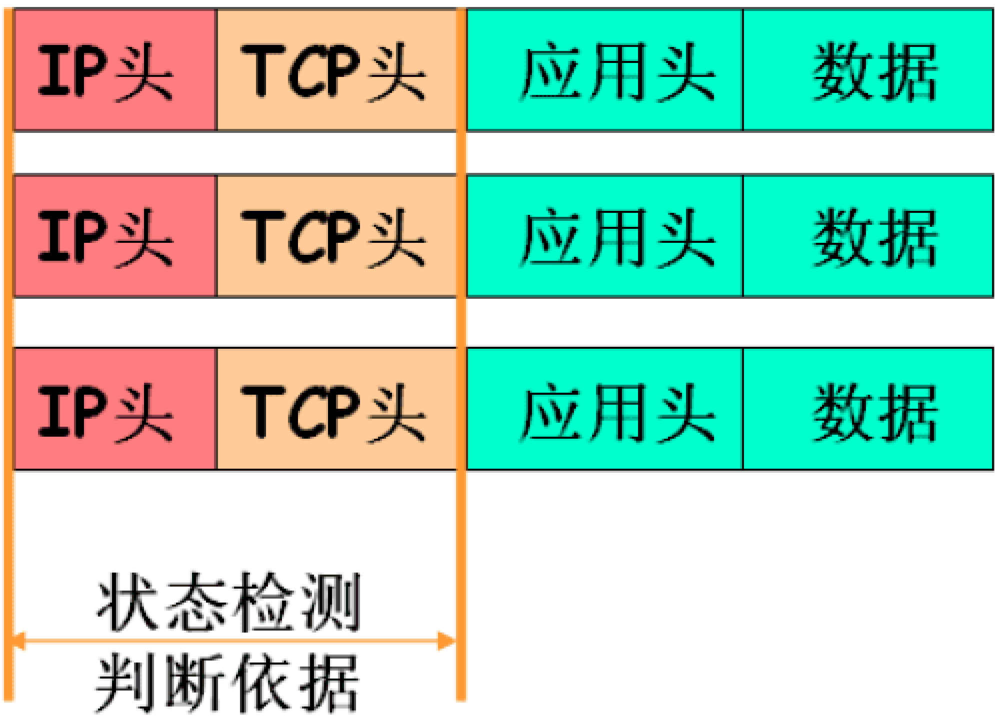


图 11-7　状态检测防火墙需要了解多个数据包之间的联系

包过滤防火墙的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。其弱点主要在于，过滤判别的依据只是网络层和传输层的有限信息，对各种具体应用的安全需求不能充分满足。其次，在部分包过滤防火墙产品中，过滤规则的数目是有限制的，而且随着规则数目的增加，性能会受到较大影响。由于缺少上下文关联信息，包过滤防火墙不能有效地过滤如 UDP、RPC(远程过程调用)一类的协议。此外，大多数包过滤防火墙中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，包过滤防火墙通常是和应用网关配合使用，共同组成防火墙系统。

(2) 应用代理(Application Proxy)防火墙

应用代理防火墙是工作应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。在应用代理防火墙技术的发展过程中，它也经历了两个不同的版本，即第一代应用网关型代理防火墙和第二代自适应代理防火墙。

第一代应用网关(Application Gateway)型防火墙是通过一种代理(Proxy)技术参与一个 TCP 连接的全过程。从内网发出的数据包经过这样的防火墙处理后，就好像是源于防火墙出口(外网)网卡一样，从而可以达到隐藏内网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

第二代自适应代理(Adaptive Proxy)型防火墙是近几年才得到广泛应用的一种新防火墙类型。它可以结合应用网关防火墙的安全性和包过滤防火墙的高速度的优点，在不损失安全性的基础之上显著提高应用代理防火墙的性能。组成这种类型防火墙的基本要素有两个，自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet Filter)。在自适应代理服务器与动态包过滤器之间存在一个控制通道。对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过 Proxy 的相应管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

应用代理防火墙的突出优点是安全。由于它工作于网络协议层的最高层，所以它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外应用代理防火墙采取是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内外网络之间的通信不是直接的，都需先经过代理服务器审核，通过后再由代理服务器代为连接，内网、外网计算机无法直接建立连接，从而避免了入侵者使用数据驱动型攻击(如缓冲区溢出攻击等)入侵内网。

应用代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网之间网关的吞吐量要求比较高时，代理防火墙容易成为内外部网络间的瓶颈。因为应用代理防火墙工作时，需要为各种类型的网络服务设置专门的代理服务，不同的代理服务为内网、外网用户建立连接、分析服务类型、过滤服务数据均会造成一定开销，因而给系统性能带来了一些负面影响。

3. 按防火墙部署位置划分

按应用部署位置的不同，防火墙可以分为边界防火墙、个人防火墙和混合式防火墙三大类。

(1) 边界防火墙

这是最为典型的防火墙部署类型，它们在内、外部网络的边界，用于对内网、外网实施隔离，保护网络边界及内部网络。这类防火墙一般都是硬件类型的，价格较贵，性能较好。边界防火墙部署示意图如图 11-8 所示。

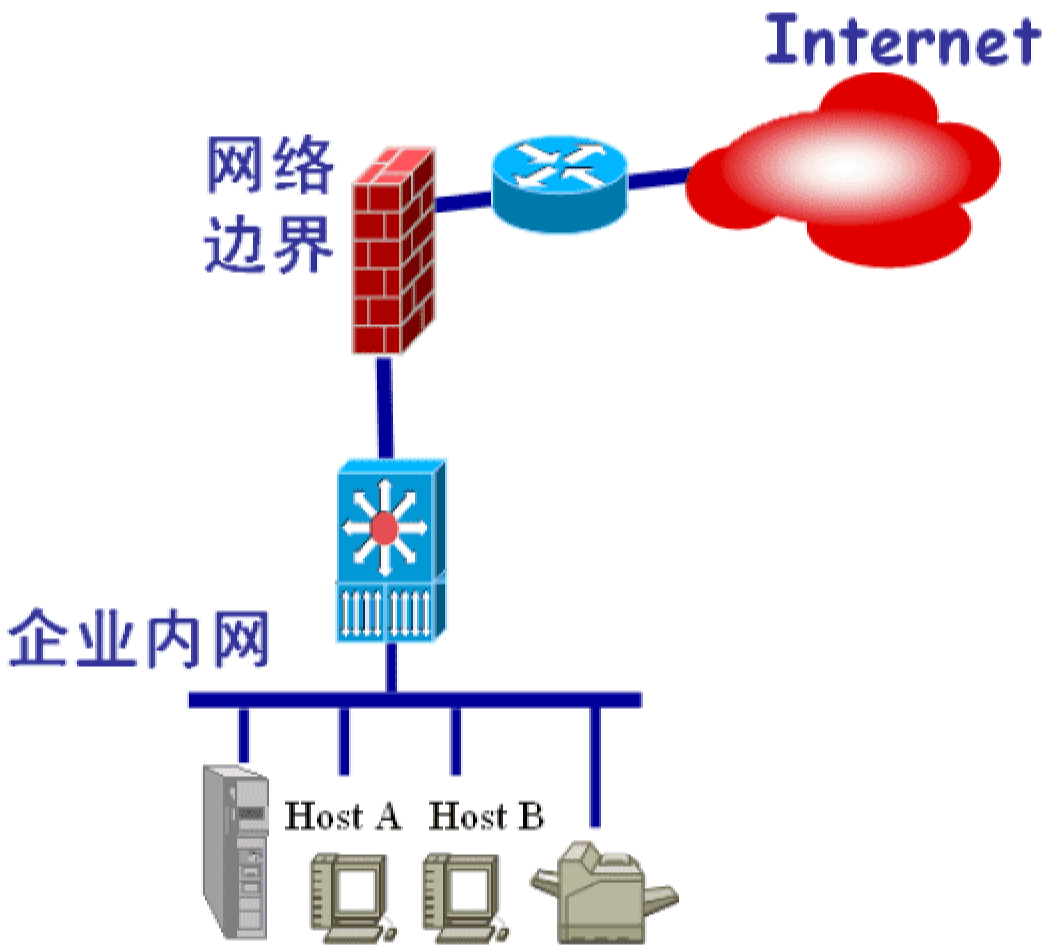


图 11-8　边界防火墙部署示意图

(2) 个人防火墙

又称单机防火墙，安装于单台主机中，防护的也只是单台主机。这类防火墙应用于广大的个人用户，通常为软件防火墙，价格最便宜，性能也最差。

(3) 混合式防火墙

即“分布式防火墙”，又称“嵌入式防火墙”，它是一整套防火墙系统，由若干个软、硬件组件组成，分布于内网、外网边界和内网中各主机之间，既对内、外网之间通信进行过滤，又对网络内部各主机间的通信进行过滤。混合式防火墙属于最新的防火墙类型，性能最好，价格也最贵。

4. 按体系结构划分

按体系结构的不同，防火墙可分为双宿主机防火墙、屏蔽主机防火墙、屏蔽子网防火墙三种。

(1) 双宿主机防火墙

又称为双重宿主主机防火墙，这类防火墙的体系结构围绕双重宿主主机构筑。双重宿主主机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器，将数据包从一个网络传送到其他网络。需要注意的是，数据包并不是从一个网络(如外网)直接发送到另一个网络(如内网)。外网能与双重宿主主机通信，内网也能与双重宿主主机通信，但是外网与内网之间的所有通信必须经过双重宿主主机的过滤和控制。

(2) 屏蔽主机防火墙

屏蔽主机防火墙使用一个屏蔽路由器把内部网络和外部网络隔离开。在这种体系结构中，安全保障由包过滤提供(例如，过滤数据包防止人们绕过代理服务器直接相连)。这种体

系结构涉及“堡垒主机”的概念。堡垒主机位于内网，是唯一能从 Internet 连接进内网的主机。任何外网的主机要访问内网的服务或资源，都必须先连接到这台主机。因此堡垒主机要保持更高等级的主机安全。

(3) 屏蔽子网防火墙

屏蔽子网防火墙添加额外的安全层到屏蔽主机防火墙中，通过添加一个独立的局域网，进一步把内网和外网(通常是 Internet)隔离开。屏蔽子网防火墙的最简单的形式为两个屏蔽路由器，每一个都连接到独立局域网。一个位于独立局域网与内网之间，另一个位于独立局域网与外网之间，这样就在内网与外网之间形成了一个“隔离带”。入侵这种防火墙保护的内部网络，攻击者必须通过两个路由器。攻击者即使入侵了堡垒主机，还必须通过内部路由器。屏蔽子网防火墙原理示意图见图 11-9。

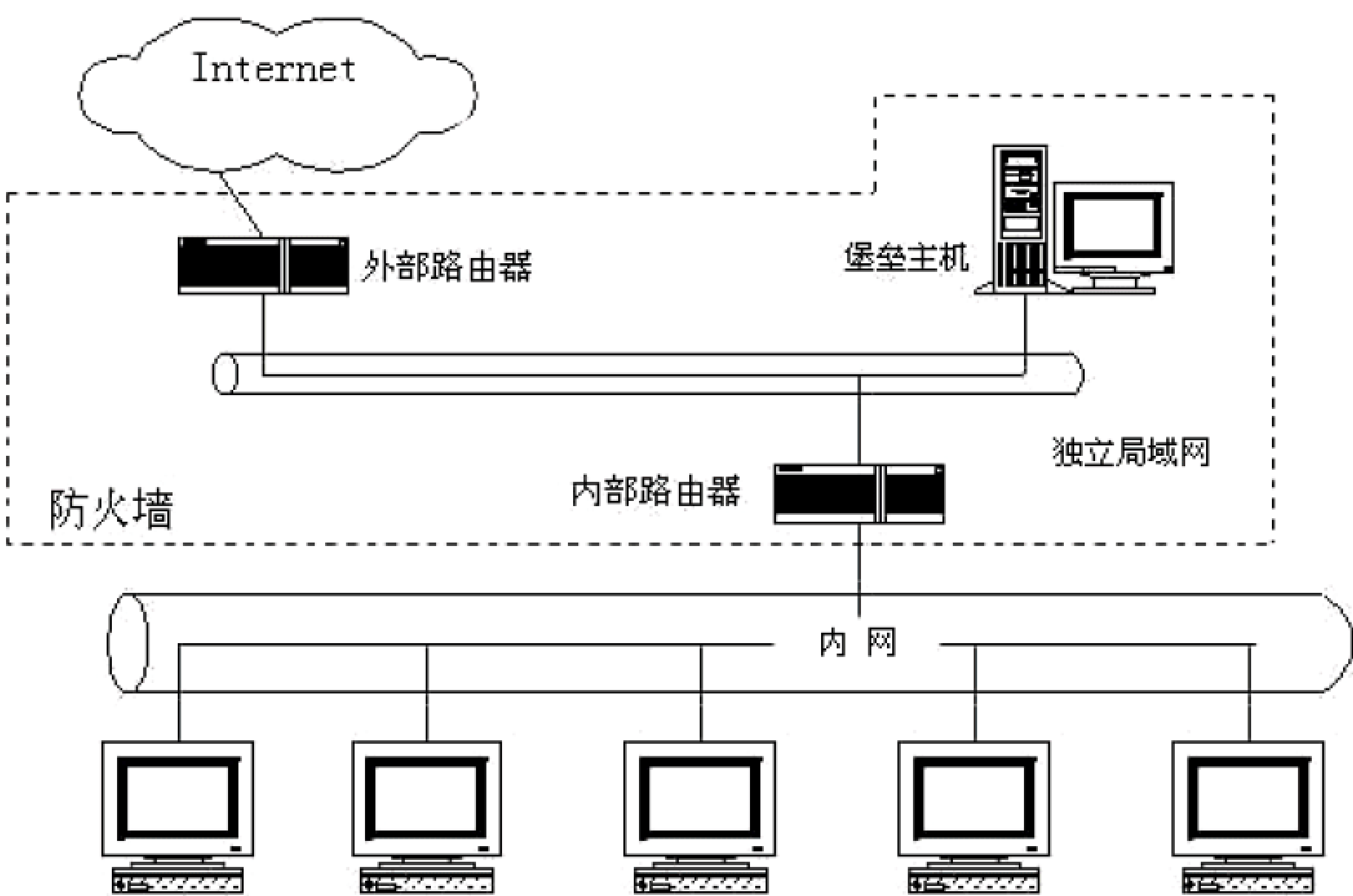


图 11-9　屏蔽子网防火墙部署示意图

5. 按防火墙实体组成划分

按实体组成来划分，防火墙主要有单一主机防火墙、路由器集成式防火墙和分布式防火墙三种。

(1) 单一主机防火墙

这是最为传统的防火墙，独立于其他网络设备，位于网络边界。这种防火墙其实与一台计算机结构类似，包括主板、CPU、内存、硬盘等基本组件。它与一般计算机最主要的区别就是一般防火墙都集成了两个以上的以太网卡，因为它需要连接至少两个及两个以上的网络。其中硬盘用于存储防火墙所用的基本程序，如包过滤程序和代理服务程序等，有的防火墙还把日志记录也记录在此硬盘上。与我们平常的 PC 机另一个重要的区别是，它要具备非常高的稳定性、实用性，具备非常高的系统吞吐性能。

(2) 路由器集成式防火墙

随着防火墙技术的发展及应用需求的提高，原来作为单一主机的防火墙已发生了许多变化。最明显的就是许多中、高档的路由器中已集成了防火墙功能。原来单一主机的防火墙由

于价格非常昂贵，仅有少数大型企业才能承受得起，为了降低企业网络投资，在中、高档路由器中集成防火墙功能，这样企业就不用再同时购买路由器和防火墙，大大降低了网络设备购买成本。典型的路由器集成式防火墙有 Cisco IOS 防火墙系列，但这种防火墙通常是较低级的包过滤型。

(3) 分布式防火墙

有的防火墙不仅是一个独立的硬件实体，而是由多个软、硬件组成的系统，又称“分布式防火墙”。分布式防火墙也不只是位于网络边界，而是作用于网络的每一台主机，对整个内部网络的主机实施保护。在网络服务器中，通常会安装一个用于防火墙系统的管理软件，在服务器及各主机上安装有集成网卡功能的 PCI 防火墙卡，防火墙卡同时兼有网卡和防火墙的双重功能。这样一个防火墙系统就可以彻底保护内部网络。各主机把任何其他主机发送的通信连接都视为“不可信” 的，都需要严格过滤。而不像传统边界防火墙那样，仅对外部网络发出的通信请求看做“不信任”。

11.3　入侵检测系统

入侵检测系统(Intrusion Detection System，IDS)是一种主动的网络安全防护措施，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击。对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统(包含程序、文件和硬件设备等)的任何变更，还能给网络安全策略的制订提供指导。更为重要的是，它易管理、配置简单，从而使非专业人员也能获得安全保障。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。

11.3.1　入侵检测系统概述

入侵不仅包括攻击者取得未授权的系统控制权，也包括收集漏洞信息，造成拒绝访问等对系统造成危害的行为。

入侵检测是对入侵行为的发觉。它通过在计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

入侵检测系统指的是有能力检测系统或网络状态改变的软、硬件的集合，它能发送警报或采取预先设置好的行动来帮助保护网络及系统。IDS 可以是一台简单的主机，例如 Unix / Linux 系统中的 tcpdump 程序可以用来获取网络状态。也可以是一个复杂的系统，使用多台主机来帮助捕获、处理并分析网络流量，例如 Linux 系统中的网络入侵检测系统 Snort IDS 等。

与其他安全产品不同的是，入侵检测系统需要更智能化，它必须将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全的运行。因此，入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现。

- 监视、分析用户及系统活动。
- 系统构造和弱点的审计。
- 识别反映已知进攻的活动模式并向相关人士报警。
- 异常行为模式的统计分析。
- 评估重要系统和数据文件的完整性。
- 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

11.3.2　入侵检测系统模型及框架

入侵检测系统模型主要分为以 Denning 模型为代表的早期 IDS 技术，以及统计学理论与专家系统相结合的标准化模型两大类。

1. IDES

1980 年 James P.Anderson 为美国空军做的一份题为《Computer Security Threat Monitoring and Surveillance，计算机安全威胁监控与监视》的技术报告中指出，审计记录可以用于识别计算机滥用(Misuse)，他给安全威胁进行了分类，第一次详细阐述了入侵检测的概念。1984—1986 年，乔治敦大学的 Dorothy Denning 和 SRI 公司计算机科学实验室的 Peter Neumann 研究出了一个实时入侵检测系统模型——入侵检测专家系统(Intrusion Detection Expert Systems，IDES)，该模型是第一个在应用中运用了统计和基于规则匹配两种技术的系统，是入侵检测系统研究中最有影响的一个系统。1989 年，加州大学戴维斯分校的 Todd Heberlein 写了一篇论文《A Network Security Monitor，网络安全监控》，该监控器用于捕获 TCP/IP 数据包，第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控不同种类主机，网络入侵检测系统自此诞生。

IDES 模型基于这样的假设：有可能建立一个框架来描述发生在主体(通常是用户)和客体(通常是文件、程序或设备)之间的正常的交互作用。这个框架由一个使用规则库(规则库描述了已知的违例行为)的专家系统支持。这能防止使用者逐渐训练(误导)系统把非法的行为当成正常的来接受，也就是说让系统“见怪不怪”。

该系统包括一个异常检测器和一个专家系统，分别用于异常模型的建立和基于规则的特征分析检测。系统的框架如图 11-10 所示。

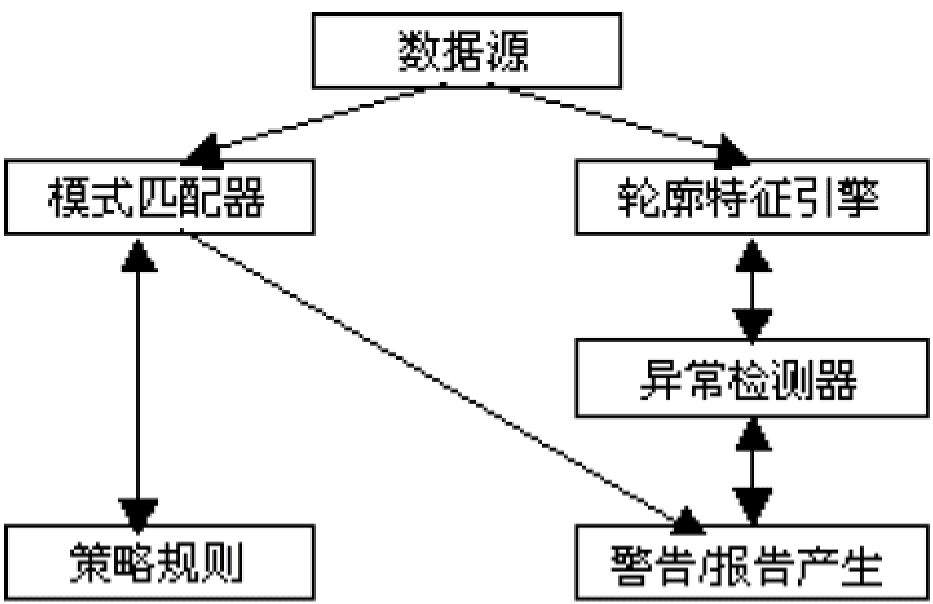


图 11-10　IDES 结构框架

2. CIDF

为解决入侵检测系统之间的互操作性，一些国际研究组织开展了标准化工作。目前对 IDS 进行标准化工作的组织有两个：IETF 的 Intrusion Detection Working Group(IDWG)和 Common Intrusion Detection Framework(CIDF)。CIDF 早期由美国国防部高级研究计划署(Advanced Research Projects Agency，ARPA)赞助研究，现在由 CIDF 工作组负责，该工作组是一个开放组织。CIDF 阐述了一个入侵检测系统(IDS)的通用模型。它将一个入侵检测系统分为以下组件：事件产生器(Event Generators)，用 E 盒表示；事件分析器(Event Analyzers)，用 A 盒表示；

响应单元(Response Units)，用 R 盒表示；事件数据库(Event Databases)，用 D 盒表示。CIDF 的结构框架如图 11-11 所示。

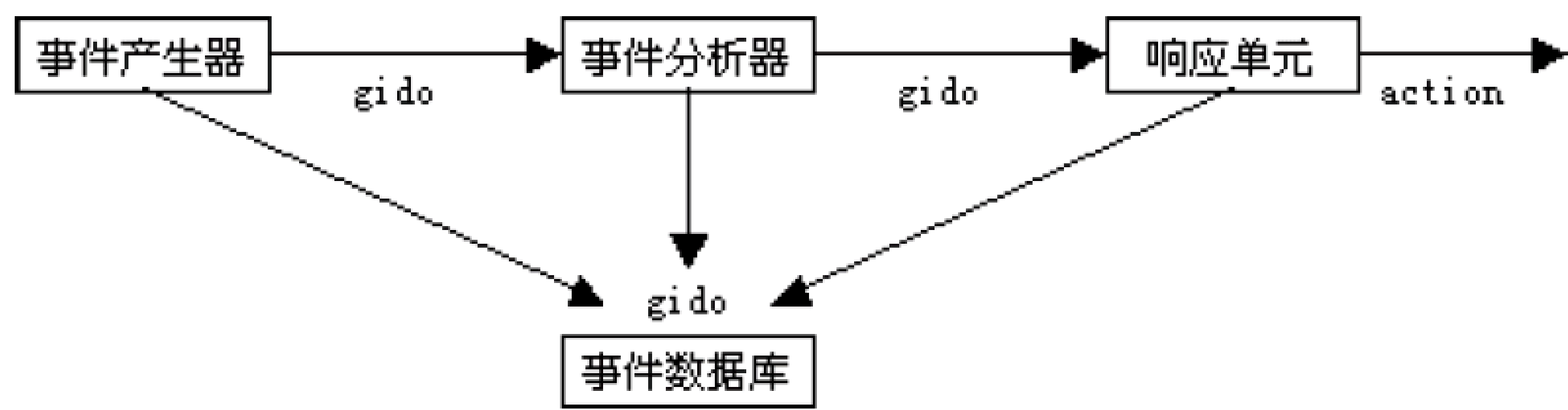


图 11-11　CIDF 结构框架

CIDF 模型的工作流程如下：E 盒通过传感器收集事件数据，并将信息传送给 A 盒，A 盒检测滥用模式；D 盒存储来自 A、E 盒的数据，并为额外的分析提供信息；R 盒从 A、E 盒中提取数据，D 盒启动适当的响应。A、E、D 以及 R 盒之间的通信规范都基于通用入侵检测对象(Generalized Intrusion Detection Objects，GIDO)。GIDO 是对事件进行编码的标准通用格式。

为了描述组件之间传送的信息，以及对这些信息进行编码的协议，CIDF 定义了公共入侵规范语言(Common Intrusion Specification Language，CISL)。CISL 可以表示 CIDF 中的各种信息，如原始事件信息、分析结果、响应提示等。如果想在不同种类的 A、E、D 及 R 盒之间实现互操作，需要实现对 GIDO 的标准化并使用 CISL。

11.3.3　入侵检测系统分类

根据对收集到的信息进行识别和分析原理的不同，可以将入侵检测分为异常检测和滥用(又称误用)检测。

异常检测(Anomaly Detection)类入侵检测系统检测目标行为与可接受行为之间的偏差。如果可以定义每项可接受的行为，那么每项不可接受的行为就应该是入侵。首先总结正常操作应该具有的特征(用户轮廓)，当用户活动与正常行为有重大偏离时即被认为是入侵。如果系统错误地将异常活动定义为入侵，则称为误报(False Positive)；如果系统未能检测出真正的入侵行为，则称为漏报(False Negative)。图 11-12 所示的是异常检测技术的模型。这种检测模型漏报率低，误报率高。因为不需要对每种入侵行为进行定义，所以能有效检测未知的入侵。

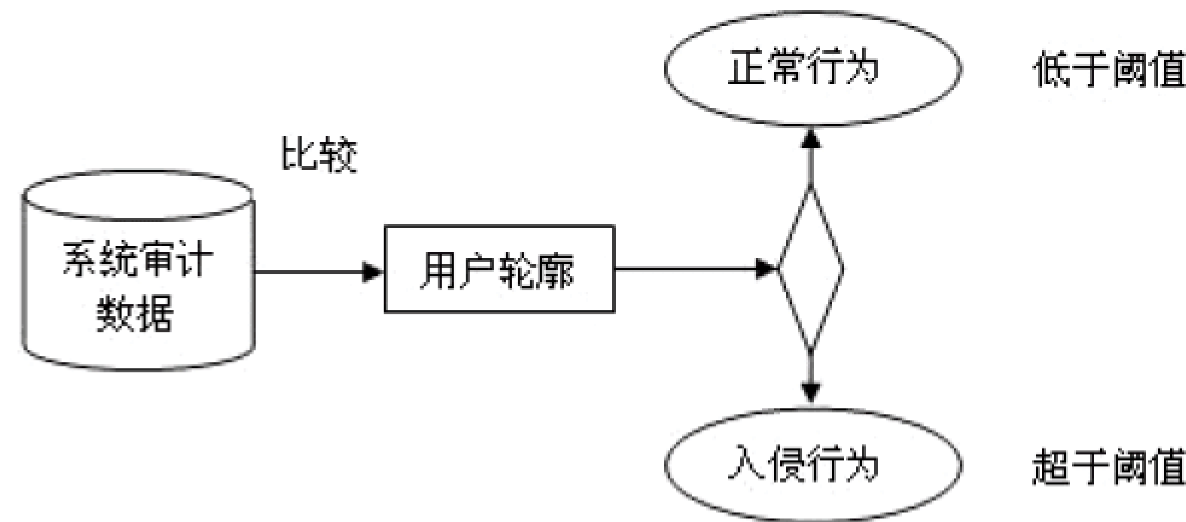


图 11-12　异常检测模型

滥用检测(Misuse Detection)类入侵检测系统检测与已知的不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为，那么每种能够与之匹配的行为都会引起告警。收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。这种检测模型误报率低、漏报率高。对于已知的攻击，它

可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且特征库必须不断更新。滥用检测模型见图 11-13 所示。

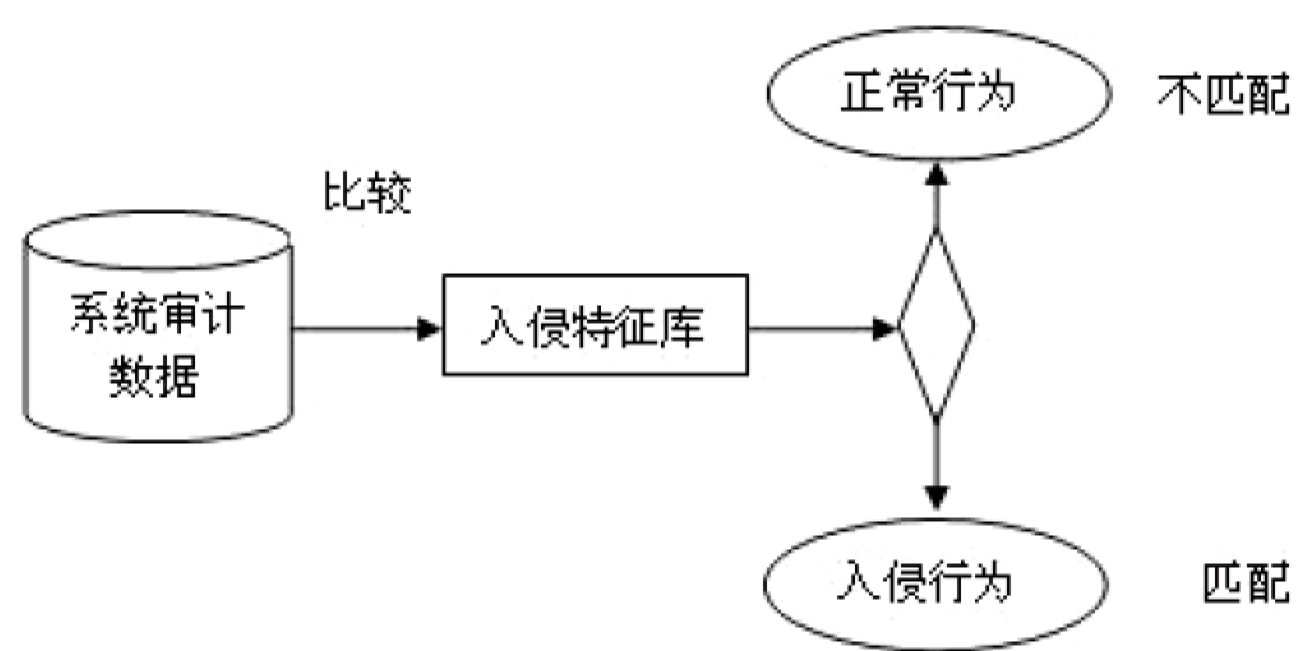


图 11-13　滥用检测模型

按照入侵检测系统的检测对象划分，入侵检测系统可分为基于主机的入侵检测系统、基于网络的入侵检测系统、分布式入侵检测系统。

1. 主机型入侵检测系统(Host Intrusion Detection System，HIDS)

系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的一般是所在的主机系统，由代理(Agent)来实现，代理是运行在目标主机上的小的可执行程序，它们与命令控制台(Console)通信。

HIDS 的优点主要如下。

- 能够监视特定的系统行为。HIDS 能够监视所有的用户登录和退出，甚至用户所做的所有操作，日志里记录的审计系统策略的改变，关键系统文件和可执行文件的改变等。
- HITDS 能够确定攻击是否成功。由于使用含有已经发生事件的信息，它们可以比网络入侵检测系统更加准确地判断攻击是否成功。
- 有些攻击在网络数据中很难发现，或者根本没有通过网络而在本地进行。这时网络入侵检测系统将无能为力，只能借助 HIDS。HIDS 的结构如图 11-14 所示。

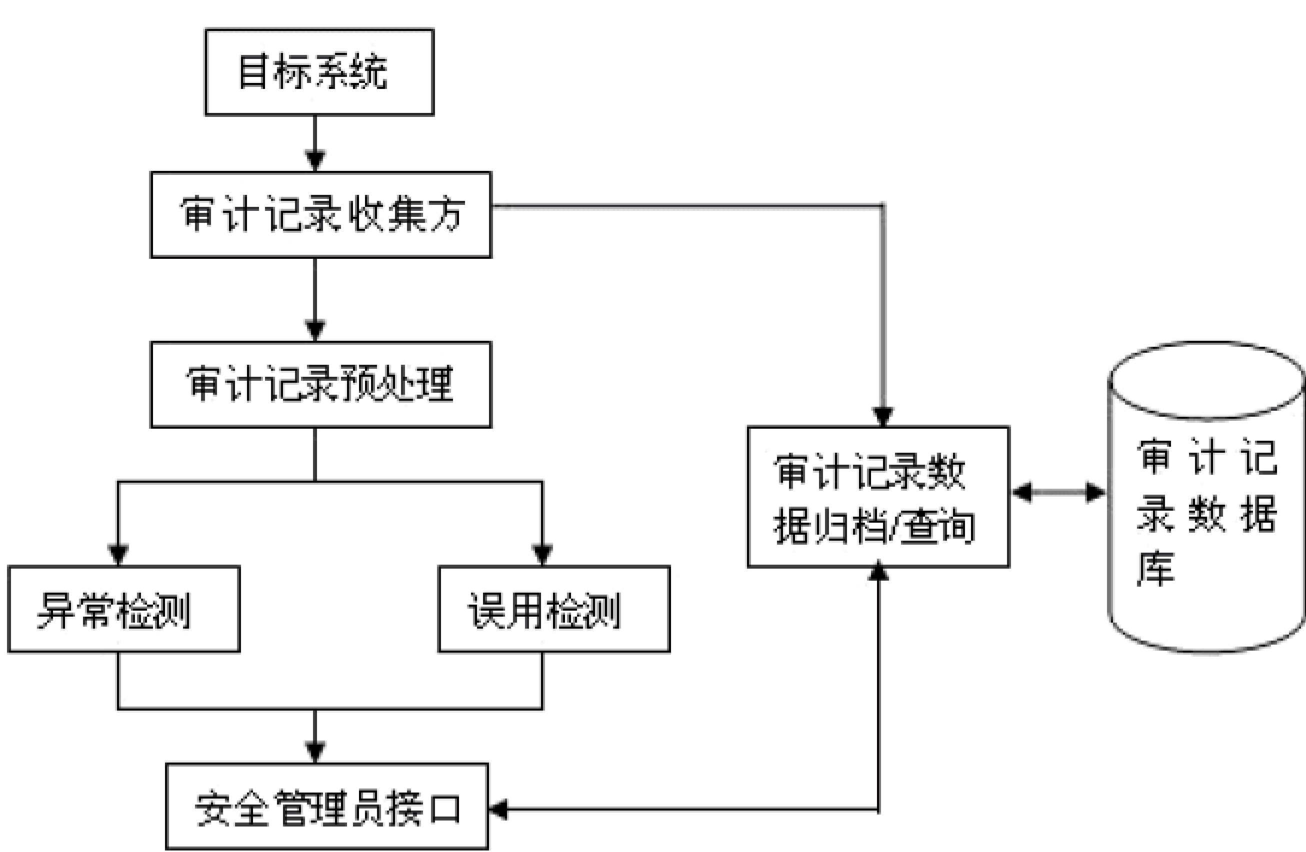


图 11-14　HIDS 结构

HIDS 的缺点主要是：一方面 HIDS 安装在需要保护的设备上，这会降低应用系统的效率。它依赖于服务器固有的日志和监视能力，如果服务器没有配置日志功能，则必须重新配置；此外全面部署 HIDS 的代价太大，维护升级不方便。

2. 网络型入侵检测系统(Network Intrusion Detection System，NIDS)

系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务，基于网络的入侵检测系统由遍及网络的采集器组成，采集器是一台将以太网卡置于混杂模式的计算机，用于嗅探网络上的数据包。探测器按一定的规则从网络上捕获与安全事件相关的数据包，然后传递给分析引擎进行安全分析判断。分析引擎从采集器上接收到数据包后结合入侵特征规则库进行分析，并把分析的结果传递给配置构造器。配置构造器按分析引擎器的分析结果构造出采集器所需要的配置规则。一旦检测到了攻击行为，NIDS 的响应模块就做出适当的响应，比如报警、切断相关用户的网络连接等。不同入侵检测系统在实现时采用的响应方式也可能不同，但通常都包括通知管理员、切断连接、记录相关的信息以提供必要的法律依据等。

NIDS 的优点是：成本低，可以检测到 HIDS 检测不到的攻击行为；入侵者消除入侵证据困难；不影响操作系统的性能；架构网络型入侵检测系统简单。其缺点是：如果网络流量很大，可能会丢失许多封包，容易让入侵者有机可乘；无法检测加密的封包；无法直接检测出对主机的入侵。需要注意的是，NIDS 只检查与它直接连接的网段的通信，不能检测在不同网段的网络包，或者说网络入侵检测系统只能工作在共享式以太网中，而在交换式以太网或者虚拟局域网(VLAN)中不能正确地工作，因为在交换式以太网或者虚拟局域网中，网络数据不会像在基于集线器的以太网中那样广播发送。交换式以太网中捕获网络数据通常采用配置交换机的镜像端口的方式来实现。NIDS 的结构见图 11-15 所示。

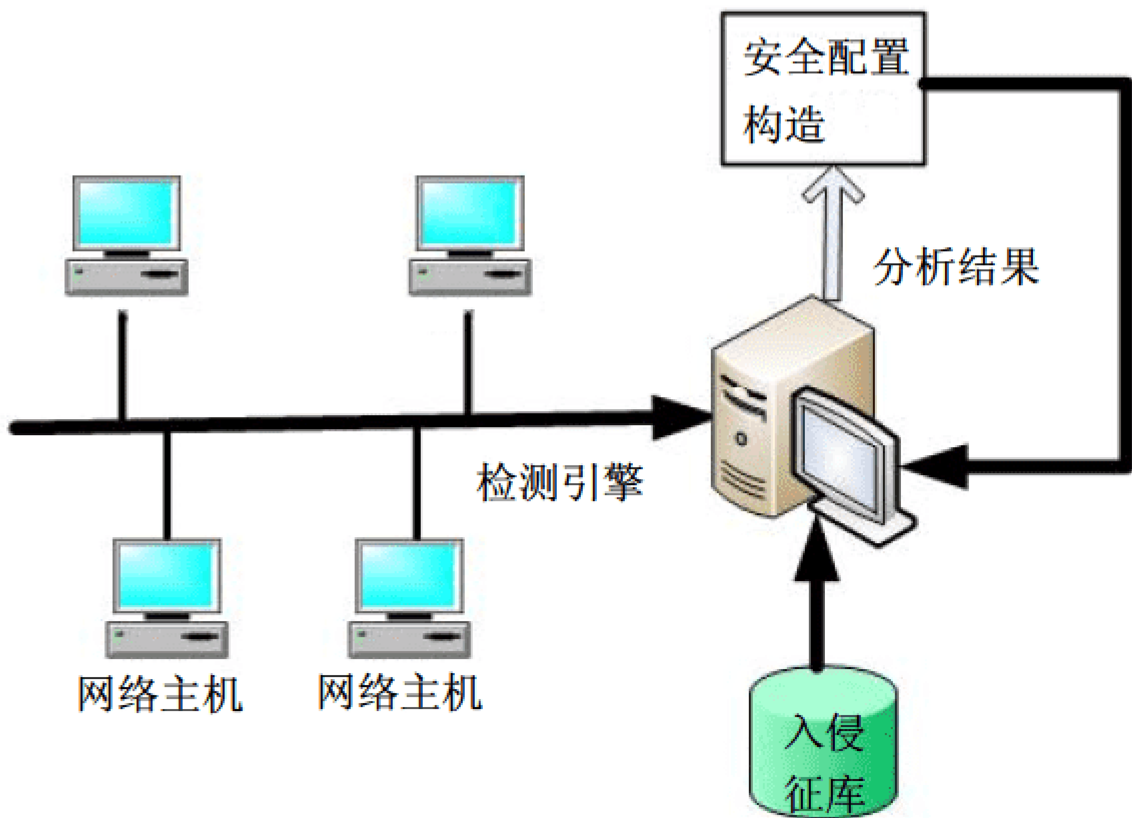


图 11-15　HIDS 结构

3. 分布式入侵检测系统(Distributed Intrusion Detection System，DIDS)

无论是 NIDS 还是 HIDS，无论采用滥用检测技术还是异常检测技术，在整个数据处理过程中，包括数据的收集、预处理、分析、检测以及检测到入侵行为后采取的相应措施，都由单个监控设备或者监控程序完成。在面临大规模、分布式的应用环境时，传统的单机方式遇到了极大的挑战。在这种情况下，要求各个 IDS 之间能够实现高效的信息共享和协作检测。在大范围网络中部署有效的 IDS 推动了分布式入侵检测系统的诞生和不断发展。在分布式入侵检测系统中，不仅数据收集组件是分布的，数据处理组件数量也应与网络中被监测主机的数量成正比。数据处理组件要处理众多数据收集组件发送来的数据，因此，要有较强的处理能力和网络吞吐能力。DIDS 一般具有图 11-16 所示的结构。

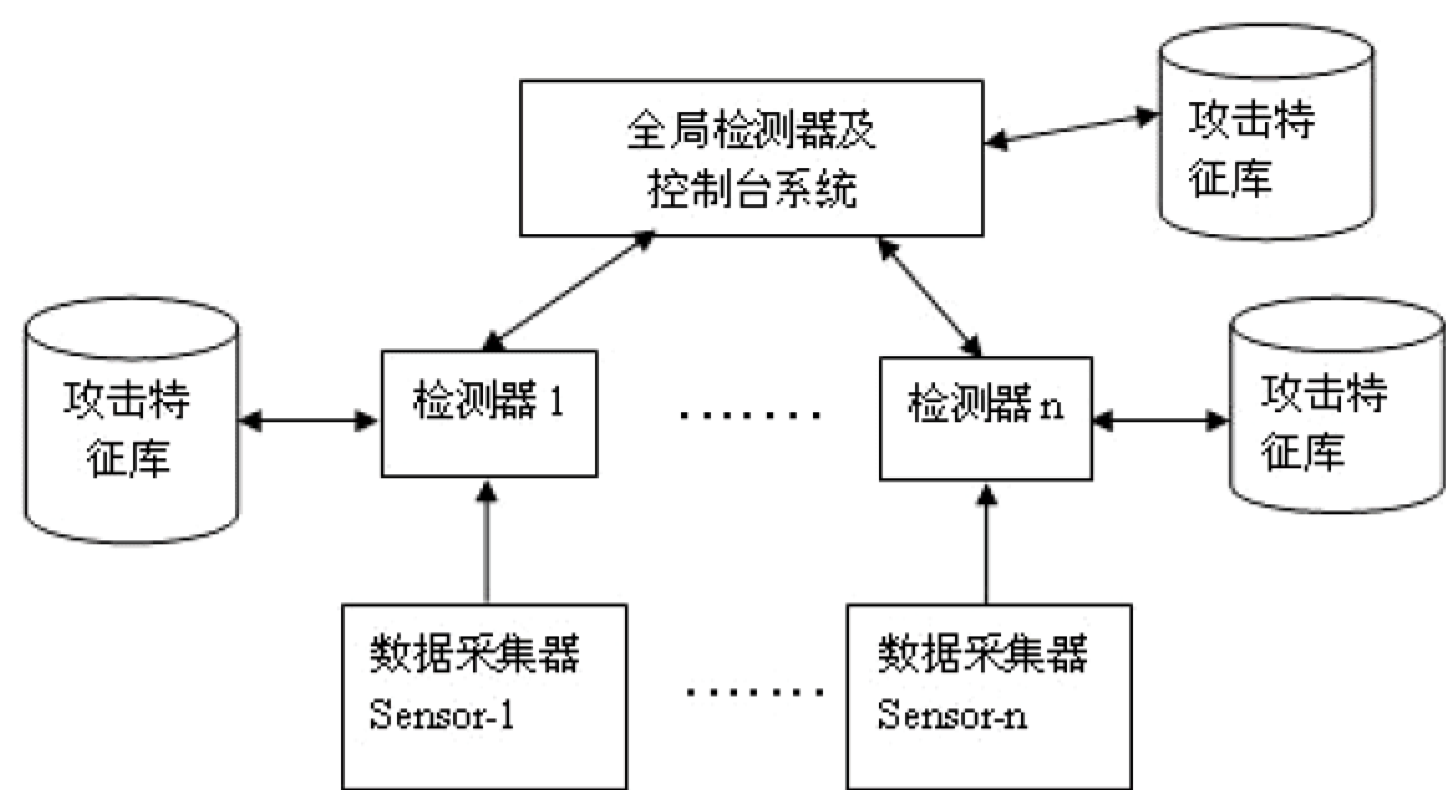


图 11-16　DIDS 结构

分布式入侵检测系统在网络上多个检测点部署具有简单检测功能的检测代理，并在网络较安全的地方部署一个全局检测代理。这种结构的特点是将部分检测功能由中心检测器下放到局部检测代理，局部检测代理能够完成大部分本地事件的简单检测功能，而将本地检测代理无法完成检测的可疑事件上传给全局检测代理，所以大量的入侵事件不必在网络上传输，这就大大缓解了因局部检测代理和全局检测器之间相互通信而对网络带宽的大量占用情况，也降低了因部署检测系统而对网络系统本身性能造成的影响。由于全局检测器能够收集到多个检测代理报告的可疑入侵事件，所以它能够在更高的层次上完成分布式、协同式的攻击检测。在系统本身的安全方面，由于各检测代理能够独立地进行本地检测，任何一个检测代理遭到攻击都不会影响其他检测代理的正常工作，增加了系统的健壮性，所以未来入侵检测技术发展的方向是采用基于代理的分布式入侵检测技术。

11.3.4　入侵检测系统部署

入侵检测系统的部署，应当遵循以下几个步骤。

1. 定义 IDS 的目标

不同的网络应用环境应当使用不同的配置规则，所以用户在配置入侵检测系统前应先明确自己的目标，建议从如下几个方面进行考虑。

- 网络拓扑需求。分析网络拓扑结构，需要监控什么样的网络，是交换式网络还是共享式网络。是否需要同时监控多个网络，多个子网是交换机连接还是通过路由器/网关连接。选择网络入口点，需要监控网络中的哪些数据流——IP 流还是 TCP/UDP 流，还是应用层的各种数据包。分析关键网络组件、网络大小和复杂度。
- 安全策略需求。是否限制 Telnet、SSH、HTTP、HTTPS 等服务管理访问。Telnet 登录是否需要登录密码。安全 Shell(SSH)认证机制是否需要加强，是否允许从非管理口(如以太网口，而不是 Console 端口)进行设备管理。
- IDS 的管理需求。哪些接口需要配置管理服务，是否启用 Telnet 进行设备管理，是否启用 SSH 进行设备管理，是否启用 HTTP 进行设备管理，是否启用 HTTPS 进行设备管理，是否需要和其他设备(例如防火墙等)进行联动。

2. 选择监视内容

- 选择监视的网络区域。在小型网络结构中，如果内部网络是可以信任的，那么只需要监控内部网络和外部网络的边界流量。
- 选择监视的数据包的类型。入侵检测系统可事先对攻击报文进行协议分析，从中提取 IP、TCP、UDP、ICMP 协议头信息和应用层的有效载荷数据的特征，并构建特征匹配规则，然后根据需求使用特征匹配规则对捕获到的网络流量(包括 IP 包、TCP 包、UDP 包和 ICMP 包)进行精确检测，若规则命中，表明该网络流量中包含入侵。
- 根据网络数据包的内容进行检测。利用字符串模式匹配技术对网络数据包的内容进行匹配以检测多种方式的攻击和探测，如缓冲区溢出、CGI 攻击、SMB 检测、操作系统类型探测等。例如，当有用户企图下载 Unix/Linux 类系统中的/etc/passwd 或/etc/shadow 文件时，IDS 也会给出警报，这是因为 IDS 捕捉到的数据包的内容中含有特征字符串/etc/passwd 或/etc/shadow。

一般来说，不同的入侵检测系统采用不同的方法来监视网络数据包的内容，例如可以采用先根据网络协议来选择入侵特征规则进行检测，然后再根据此协议数据包中的字符特征进行检测。

3. 部署 IDS

1) 只检测内部网络和外部网络边界流量

这种情况下，入侵检测系统部署在出口路由器或防火墙的后面，用来监控网络入口处所有流入和流出网络的数据，网络拓扑结构可按照图 11-17 所示的方式进行部署。

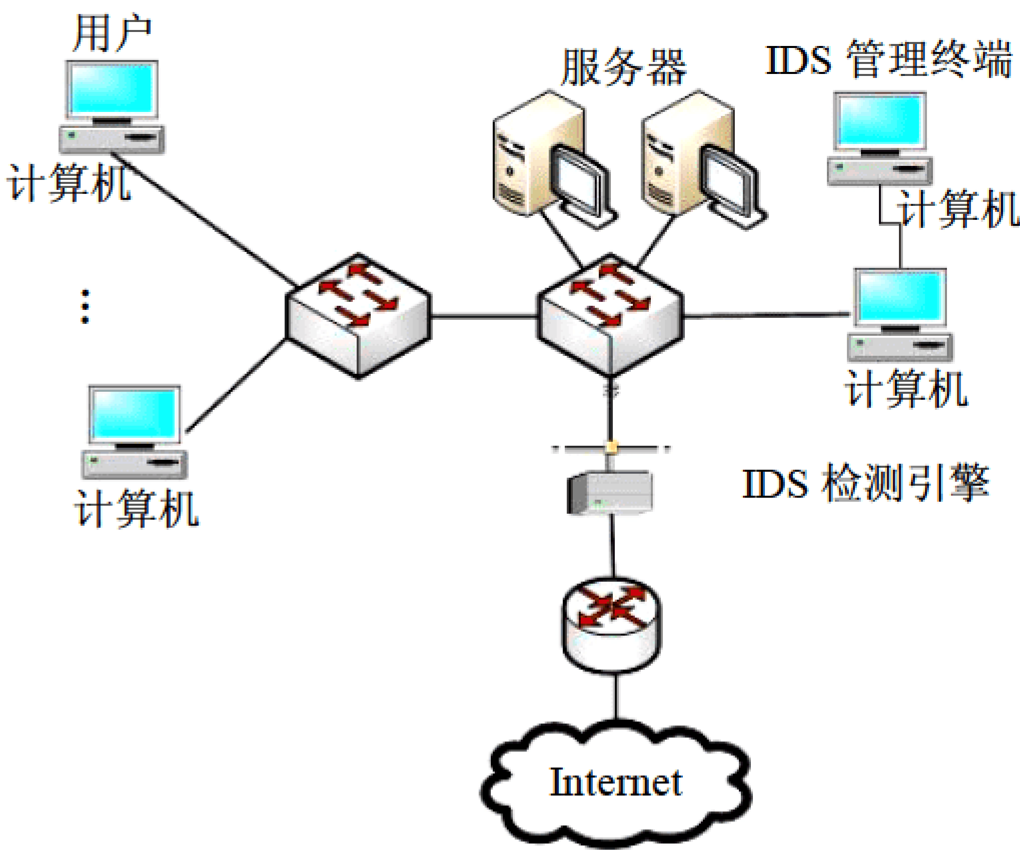


图 11-17　只监控网络边界浏览的 IDS 系统部署

在图 11-17 中，IDS 被部署在内部网络与 Internet 的出口处，IDS 设备的监听口连接到了内部网络出口处的交换机(Switch)镜像口上，从而可以捕获到交换机镜像接口的网络流量。管理员可以通过命令行方式(Console、Telnet 或 SSH)或 Web 方式(HTTP 或 HTTPS)远程登录到 IDS 管理接口并对设备进行配置管理。图 11-17 所示的部署方式不仅方便了用户的使用和配置，也节约了投资成本，适合中小规模企业的网络安全应用。

2) 集中监控多个子网流量

在这种情况下，IDS 的部署见图 11-18。内部局域网中划分了多个不同职能的子网，有些子网访问某些子网资源量希望受到监控和保护，本例假设需要对关键子网 LAN1 的流量进行监控，且 LAN2 子网放置了各种服务器，因此对 LAN2 的所有流量也需要进行监控。同时网络管理员要能够集中监控网络的流量和异常情况。

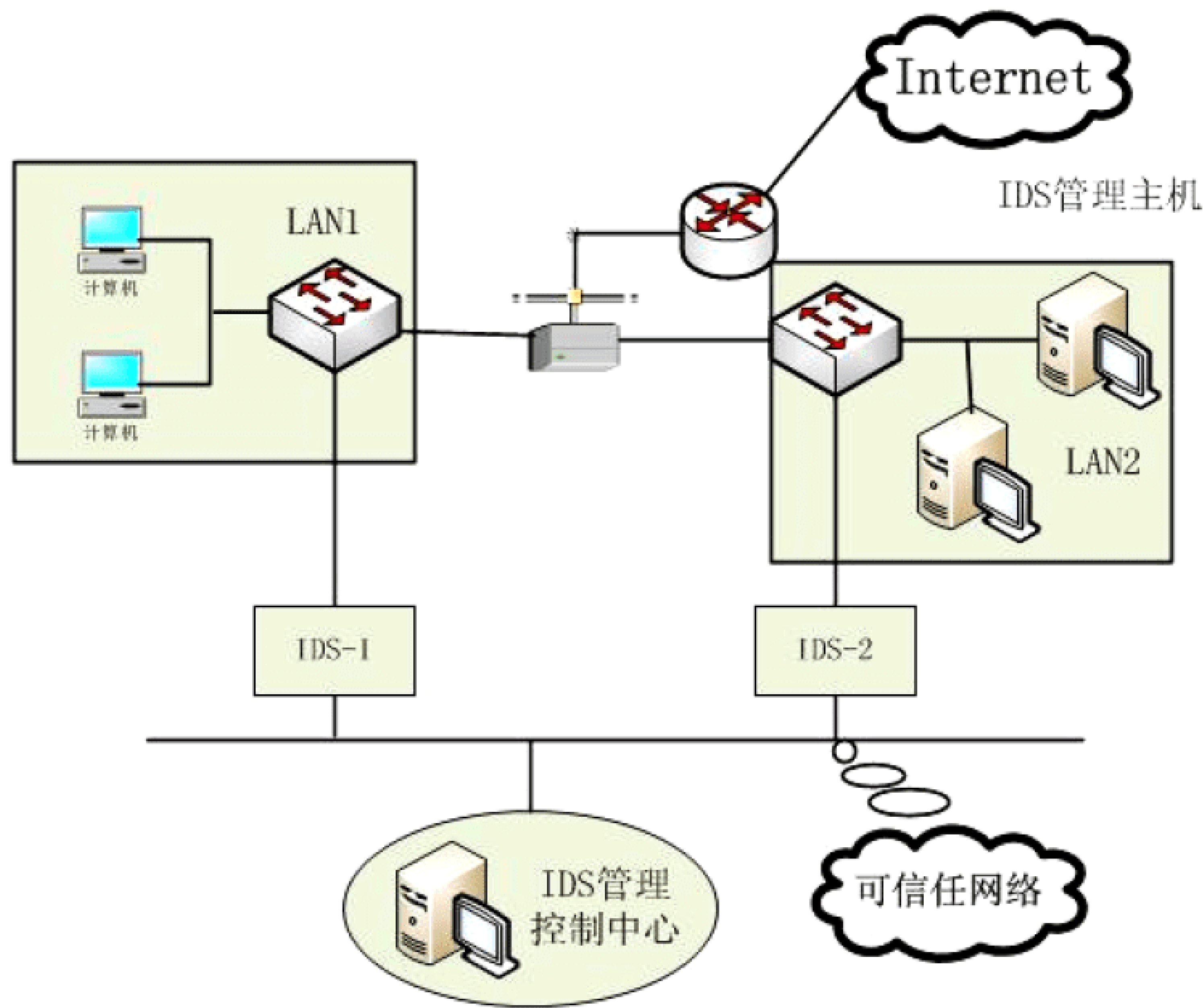


图 11-18　集中监控多个子网流量的 IDS 系统部署

管理员可以通过安全管理平台全网的 IDS 设备进行统一的配置管理、策略部署和安全事件监控，还可以安全管理平台提供的多种智能分析和管理手段对收集到的网络安全事件信息进行处理，并依据处理结果调整安全策略和防护手段，从而提高网络安全的整体水平。

11.4　VPN

虚拟专用网(Virtual Private Network，VPN)被定义为通过一个公用网络(通常是 Internet)建立一个临时的、安全的连接，是一条穿过不可信的公用网络的安全稳定的隧道。VPN 是对企业内部网的扩展。

VPN 可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网络建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的网络上，一个企业的 VPN 解决方案将大幅度减少用户花费在城域网和远程网络连接上的费用。同时，这将简化网络的设计和管理，加速连入新的用户和网站。另外，VPN 还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的 VPN 解决方案可以使用户将精力集中到自己的生意上，而不是网络上。VPN 可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网。

11.4.1　VPN 概述

VPN 是利用公共网络基础设施，通过“隧道”技术等手段实现类似私有专网的数据安全传输。VPN 具有虚拟特点，即 VPN 并不是某个公司专有的封闭线路或者是租用某个网络服务商提供的封闭线路，但同时 VPN 又具有专线的数据传输功能，因为 VPN 能够像专线一样在公共网络上处理自己公司的信息。VPN 可以说是一种网络外包，企业不再追求拥有自己的专有网络，而是将对另一个部门或分支企业的网络访问需求，部分或全部外包给一个专业公

司去做。VPN 工作原理示意图见图 11-19。

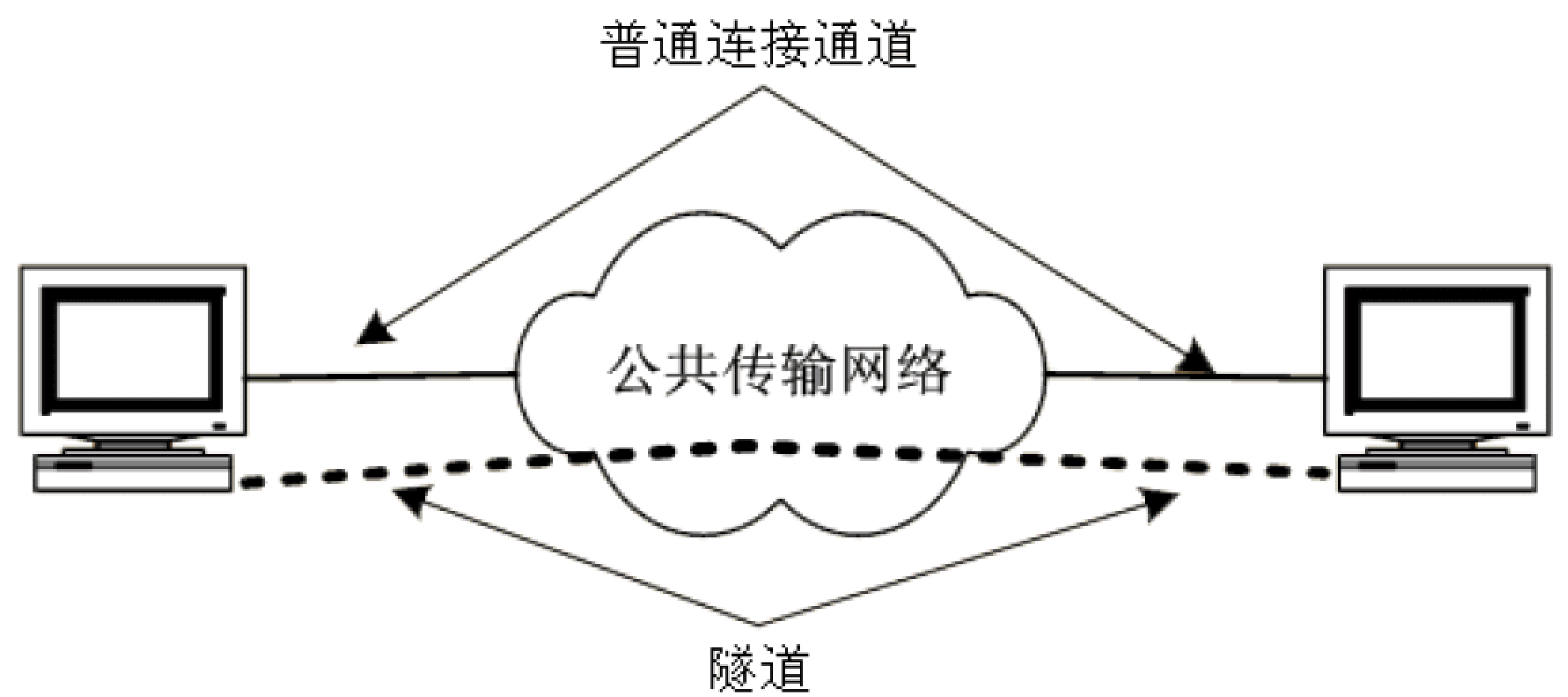


图 11-19　VPN 工作原理示意图

隧道是一种利用公网设施在一个网络之中的“网络”上传输数据的方法。隧道协议利用附加的头部信息封装帧，附加的头部提供了路由信息，因此封装后的帧能够通过中间的公用网络。封装后的帧所途经的公用网络的逻辑路径称为隧道。一旦封装的帧到达了公用网络上的目的地，帧就会被解除封装并被继续送到最终目的地。

目前很多单位都面临着这样的挑战，分公司、经销商、合作伙伴、客户和外地出差人员要求随时经过公用网访问公司的资源。这些资源包括：公司的内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。安全接入互联网的传统方法是 VPN。尽管 VPN 的安装和硬件维护需要一定的费用，但是日益增长的远距离工作和远程接入的需求使 VPN 变得十分必要。

VPN 具有以下优点。

1. 降低成本

企业不必租用长途专线建设专网，不必大量的网络维护人员和设备投资。利用现有的公用网组建的 Intranet，比租用专线或铺设专线开支少得多，而且距离越远节省的越多。例如，某企业的北京与纽约分部之间的连接，不太可能自铺专线。当一个远程用户在纽约想要连到北京的 Intranet，用拨号访问时，花的是国际长途话费。而用 VPN 技术，只需在纽约和北京分别连接到当地的 Internet 就实现了互联，双方花的都是市话费及比较低廉的本地上网费用。

2. 容易扩展

网络路由设备配置简单，无需增加太多的设备，省时省钱。对于发展很快的企业，对 VPN 的需求就更加迫切。如果企业组建自己的专用网，在扩展网络分支时，考虑到网络的容量，架设新链路，增加互联设备，升级设备等。而实现 VPN 后则方便得多，只需连接到公用网上，对新加入的网络终端在逻辑上进行设置，也不需要考虑公用网的容量问题、设备问题等。

3. 完全控制主动权

VPN 上的设施和服务完全掌握在企业手中。例如，企业可以把拨号访问交给网络服务提供商(Network Service Provider，NSP)去做，自己负责用户的查验、访问权、网络地址、安全

性和网络变化管理等重要工作。VPN 通过采用“隧道”技术，并在 IETF(Internet Engineering Task Force，Internet 工程工作组)制定的 IPSec(IP Security，IP 协议安全)统一标准下，在公众网中构造企业的安全、机密、顺畅的专用链路。

11.4.2　VPN 类型

按照不同分类方法，VPN 可分为不同类型。

(1) 按应用方式分类，VPN 有两种基本类型：拨号 VPN 与专用 VPN。

拨号 VPN 为移动用户和远程办公用户提供了对公司企业网的远程访问。这是当今最常见的一种 VPN 部署形式，主要是基于 L2F 协议。拨号 VPN 使多个不同领域的用户都能通过公共网络或者 Internet 获得安全的通路，以访问其企业内部网络。

专用 VPN 以多个用户和比拨号 VPN 高速的连接为特征。有多种形式的专用 VPN 业务，但最常见的是在 IP 网上建立的 IP VPN 业务。专用 VPN 提供了公司总部与公司分部、远程分支办事处以及 Extranet 用户的虚拟点对点连接。

完整的 VPN 解决方案通常把拨号 VPN 和专用 VPN 组合在一起，以满足不同用户的使用需求。

(2) 按应用平台分类 VPN 可分为软件平台 VPN、专用硬件平台 VPN 以及辅助硬件平台 VPN。

软件平台 VPN 用于对数据连接速率要求不高，对性能和安全性需求不强时。可以利用一些软件公司所提供的完全基于软件的 VPN 产品实现简单的 VPN 功能。

使用专用硬件平台的 VPN 设备可以满足企业和个人用户对提高数据安全及通信性能的需求，尤其是从通信性能的角度来看，指定的硬件平台可以完成数据加密等对 CPU 处理能力需求较高的功能。提供这些平台的硬件厂商比较多，如 Nortel、Cisco 等。

辅助硬件平台 VPN 介于软件平台和专用硬件平台之间，辅助硬件平台的 VPN 主要是指以现有网络设备为基础，再增添适当的 VPN 软件以实现 VPN 的功能。

(3) 按构建 VPN 的隧道协议分类。

可将 VPN 分为二层 VPN、三层 VPN。

VPN 的隧道协议可分为第二层隧道协议、第三层隧道协议。第二层隧道协议最为典型的有 PPTP、L2F、L2TP 等，第三层隧道协议有 GRE、IPSec 等。

第二层隧道协议和第三层隧道协议的本质区别在于，在隧道里传输的用户数据包被封装在哪一层的数据包中。第二层隧道协议和第三层隧道协议一般来说分别使用，但合理运用两层协议，将具有更好的安全性。

因实际使用中，需要通过客户端与服务器端的交互实现认证与隧道建立，故基于二层、三层的 VPN 都需要安装专门的客户端系统(硬件或软件)，完成 VPN 相关的工作。

(4) 按服务类型分类。

VPN 业务按用户需求分为三类：Intranet VPN、Access VPN 和 Extranet VPN。

Intranet VPN(内部网 VPN)即企业的总部与分支机构间通过公网构筑的虚拟网。这种类型的连接带来的风险最小，因为公司通常认为它们的分支机构是可信的，并将它作为公司网络

的扩展。内部网 VPN 的安全性取决于两个 VPN 服务器之间的加密和验证手段。Intranet VPN 结构图如图 11-20 所示。

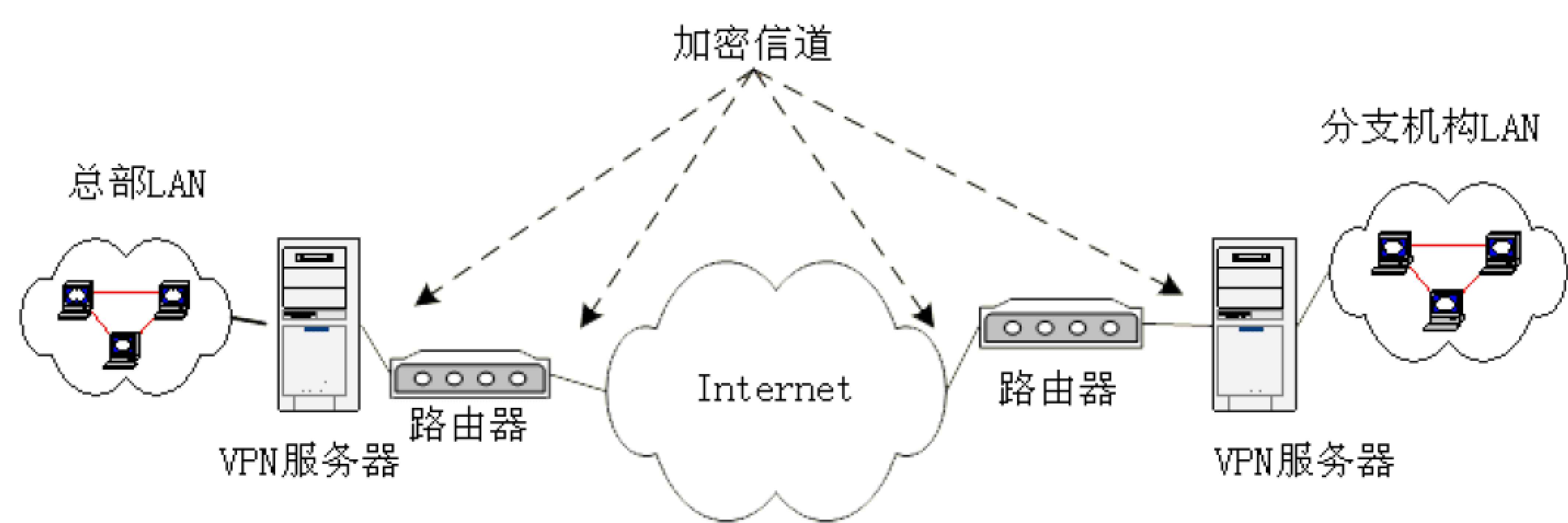


图 11-20　Intranet VPN 结构图

Access VPN(远程访问 VPN)又称为拨号 VPN(即 VPDN)，是指企业员工或企业的小分支机构通过公网远程拨号的方式构筑的 VPN。典型的远程访问 VPN 是用户通过本地的 Internet 服务提供商(Internet Service Provider，ISP)登录到 Internet 上，并在现在的办公室和公司内部网之间建立一条加密信道。Access VPN 结构图如图 11-21 所示。

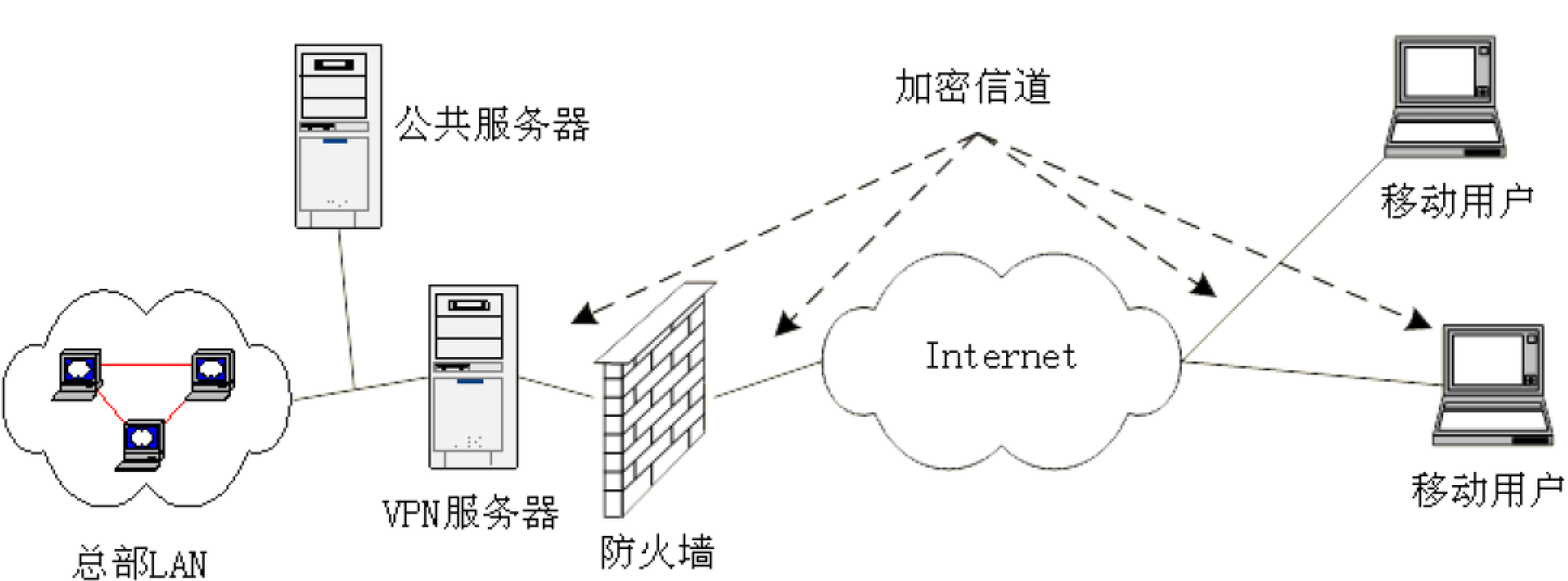


图 11-21　Access VPN 结构图

Extranet VPN(外联网 VPN)即企业间发生收购、兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的 VPN。它能保证包括 TCP 和 UDP 服务在内的各种应用服务的安全，如 WWW、Email、HTTP、FTP、RealAudio、数据库的安全以及一些应用程序如 Java、ActiveX 的安全。Extranet VPN 结构如图 11-22 所示。

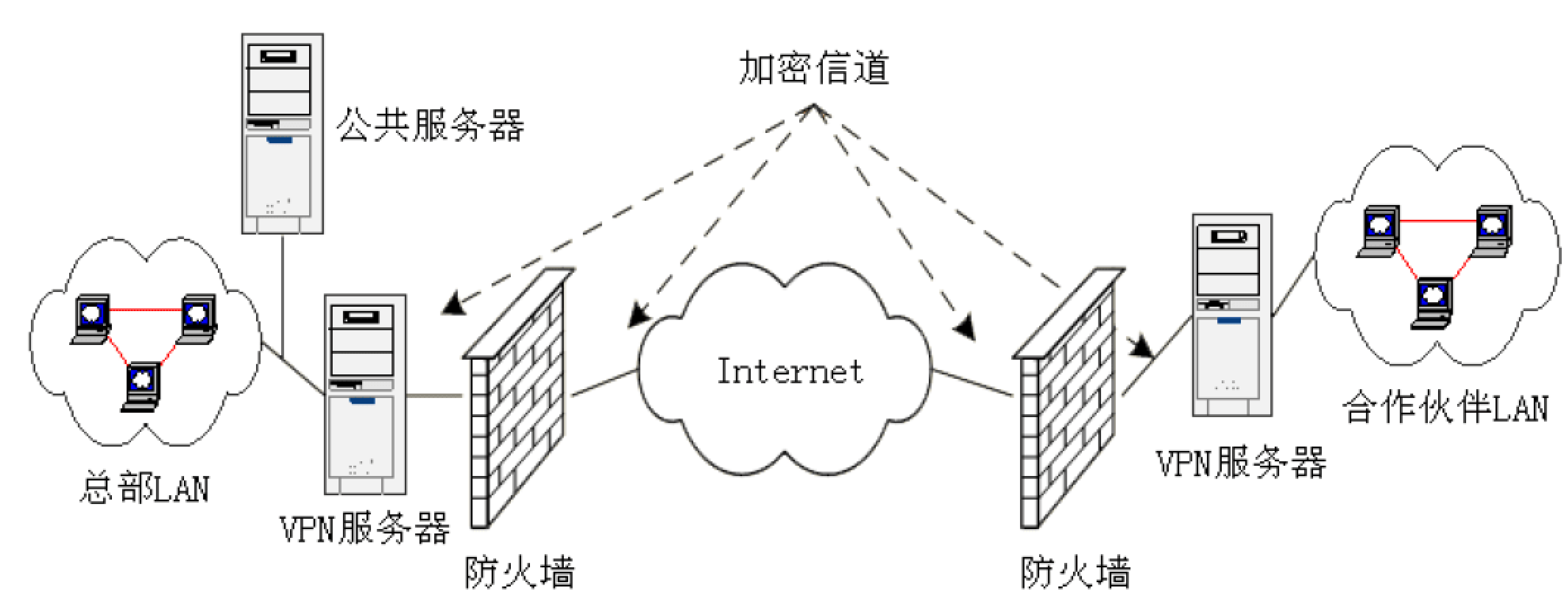


图 11-22　Extranet VPN 结构图

(5) 按 VPN 的部署模式分类。

VPN 可分为端到端(End-to-End)模式、供应商—企业(Provider-to-Enterprise)模式、内部供应商(Intra-Provider)模式。

端到端(End-to-End)模式是典型的由自建 VPN 的客户所采用的模式，最常见的隧道协议是 IPSec 和 PPTP。

供应商—企业(Provider-to-Enterprise)模式中，隧道通常在 VPN 服务器或路由器中创建，在客户前端关闭。利用该模式客户不需要购买专门的隧道软件，而由服务商的设备来建立通道并验证。最常见的隧道协议有 L2TP、L2F 和 PPTP。

内部供应商(Intra-Provider)模式中，服务商保持了对整个 VPN 设施的控制。在该模式中，通道的建立和终止都是在服务商的网络设施中实现的。客户不需要做任何实现 VPN 的工作。

11.4.3　VPN 工作原理

VPN 是利用公网来构建专用网络，它利用特殊设计的硬件和软件直接通过共享的 IP 网所建立的隧道来完成。我们通常将 VPN 当作 WAN 解决方案，但它也可以简单地用于 LAN。VPN 类似于点到点直接拨号连接或租用线路连接，尽管它是以交换和路由的方式工作。

可以说，VPN 是 Intranet 在公用网络上的延伸，它可以提供与专用网一样的安全性、可管理性和传输性能，而建设、运转和维护网络的工作也从企业内部的 IT 部门剥离出来，交由运营商来负责，从而在公共网络上创建一个安全的私有连接，让公司的远程用户、分支机构、业务伙伴等与公司的企业网连接起来，构成一个扩展的企业网。

VPN 是建立在实际网络(或物理网络)基础上的一种功能性网络。它利用公共网络作为企业骨干网的低成本优势，同时克服公共网络缺乏保密性的弱点，在 VPN 网络中，位于公共网络两端的网络在公共网络上传输信息时，其信息都是经过安全处理的，可以保证数据的完整性、真实性和私有性。

VPN 是指在共用网络上建立专用网络的技术。之所以称为虚拟网，主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网建设所需的点到点的物理链路，而是架构在公用网络服务商(ISP)所提供的网络平台之上的逻辑网络。用户的数据是通过 ISP 在公共网络(Internet)中建立的逻辑隧道(Tunnel)，即点到点的虚拟专线进行传输的。通过相应的加密和认证技术来保证用户内部网络数据在公网上安全传输，从而真正实现网络数据的专有性。利用 VPN 实现 Intranet 的扩展原理如图 11-23 所示。

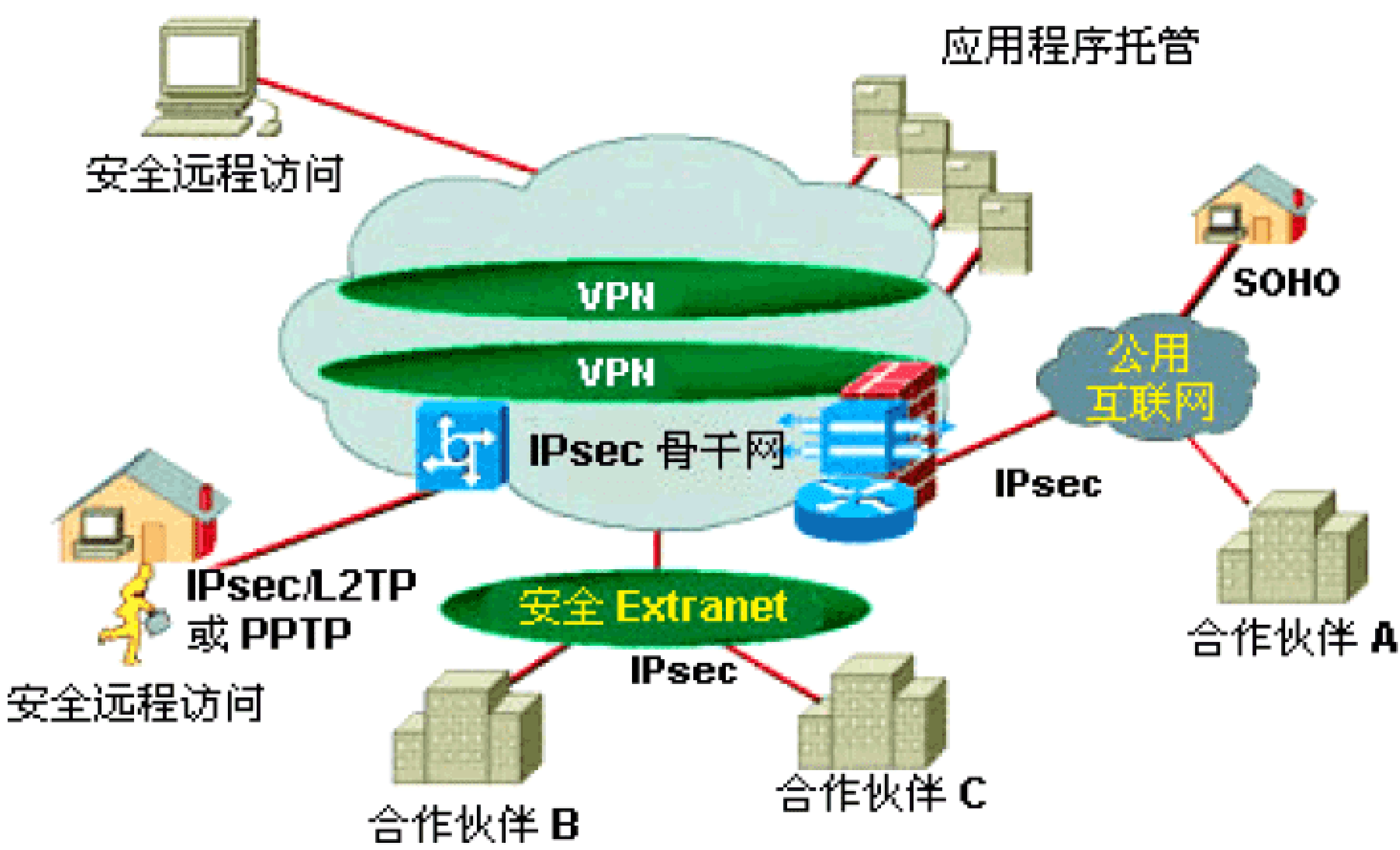


图 11-23　VPN 实现 Intranet 扩展

建立隧道有两种主要的方式：客户启动(Client-Initiated)方式或客户透明(Client-Transparent)方式。

客户启动方式要求客户和隧道服务器(或网关)都安装隧道软件。后者通常都安装在公司网络中心节点上。通过客户软件初始化隧道，隧道服务器中止隧道，ISP 可以不必支持隧道。客户和隧道服务器只需建立隧道，并使用用户 ID 和口令或用数字证书鉴权。一旦隧道建立，就可以进行通信了，如同 ISP 没有参与连接一样。

另外，如果希望隧道对客户透明，ISP 就必须具备允许使用隧道的接入服务器以及可能需要的路由器。客户首先拨号连接接入服务器，服务器必须能识别这一连接要与某一特定的远程点建立隧道，然后接入服务器与隧道服务器建立隧道，通过用户 ID 和口令进行鉴权。这样客户端就通过隧道与隧道服务器建立了直接对话。尽管这一方式不要求客户有专门软件，但客户只能拨号进入正确配置的访问服务器。

11.4.4　VPN 主要技术

在一个完整的 VPN 技术方案中，所涉及的主要技术包括隧道技术、密码技术和服务质量保证技术。密码技术详见第 5 章，这里主要介绍隧道技术和服务质量保证技术。

1. 隧道技术

隧道技术实质上是一种数据封装技术，即将一种协议封装在另一种协议中传输，从而实现被封装协议对封装协议的透明性，保持被封装协议的安全特性。使用 IP 协议作为封装协议的隧道协议称为 IP 隧道协议。利用隧道技术，理论上任何协议的数据都可以通过 IP 网络传输。

为了透明传输多种不同网络层协议的数据包，可采用以下两种方法。

一种方法是先把各种网络层协议(如 IP、IPX 和 AppleTalk 等)封装到链路层的点到点协议(PPP)帧里，再把整个 PPP 帧装入隧道协议里。这种方法封装的是 TCP/IP 协议栈链路层的数据包，称为“第二层隧道”。

另一种方法是把各种网络层协议直接装入隧道协议中，由于封装的是网络协议栈第三层网络层协议数据包，所以称为“第三层隧道”。

第二层隧道协议主要有：Microsoft、3Com 和 Ascend 公司在 PPP 基础上开发的点到点隧道协议(Point-to-Point Tunnel Protocol，PPTP)，主要用于端到端的 VPN 解决方案。Cisco 公司提出的第二层转发协议(Layer 2 Forwarding，L2F)和第二层隧道协议(Layer 2 Tunneling Protocol，L2TP)，主要用于基于路由器的虚拟专网组网方案中。它优于 PPTP 的一个特点是可以建立多点隧道。使用户可以开通多个 VPN，以便同时访问 Internet 和企业网络。L2TP、PPTP 都被集成在 Windows 操作系统中，所以最为常用。

第三层隧道协议主要有 IP 层安全协议(IP Security，IPSec)、移动 IP 协议和虚拟隧道协议(Virtual Tunnel Protocol，VTP)。其中 IPSec 应用最为广泛，成为事实上的网络层安全标准，不但符合现有的 IPv4 环境，同时也是 IPv6 环境下的安全标准。IPSec 是 IEIF IPSec 工作组为了在 IP 层提供通信安全而制定的一套协议簇，是一个应用广泛、开放的 VPN 安全协议体系，工作在网络层。IPSec 不是加密算法或认证算法，只是一个开放结构，定义了在 IP 数据包格式中，为实现数据加密或认证的相关数据结构，为算法的实现提供了统一的体系结构。不同

的加密算法都可以利用 IPSec 定义的体系结构在网络数据传输过程中实施。

2. QoS(Quality of Service，服务质量)保证技术

通过隧道技术和加密技术可以建立一个具有安全性、互操作性的 VPN。但是该 VPN 的性能可能不稳定，需要在 VPN 隧道运行的网段加入 QoS 技术。

QoS 的主要指标有：带宽，即网络提供给用户的传输率；反应时间，即用户所能容忍的数据包传输延时；抖动，即延时的变化；丢失率，即数据包丢失的比率。

QoS 机制具有通信处理机制以及供应和配置机制。通信处理机制协议体系包括 IEEE 802.1p、区分服务(Differentiated Service，DiffServ)、综合服务(Integrated Services，IntServ)等等。现有局域网大多数是基于 IEEE 802 技术的，802.1p 则为这些局域网提供了支持 Qos 的机制。供应和配置机制包括资源保留配置协议(Resource Reservation Setup Protocol，RSVP)、子网带宽管理(Subnet Bandwidth Manager，SBM)、策略机制和管理工具等。供应机制指的是比较静态、长期的管理任务，如网络设备的选择、网络设备的更新、接口的添加/删除、拓扑结构的改变等。配置机制指的是比较动态、短期的任务管理，如流量处理的参数。

本 章 小 结

本章介绍了网络安全相关的几个基本方面的技术。作为网络安全的基石，首先介绍了数据加密技术的应用模式，然后介绍了网络安全体系中要求的基础设备——防火墙、入侵检测系统。阐述了防火墙和入侵检测系统的基本概念、目的，从不同角度介绍了这些安全设备的基本工作原理以及分类方法。在具备安全保障的前提下，用于实现将企业局域网扩展至全球并的技术——VPN，是当前网络安全应用的热点内容，本章最后一节对其工作原理、分类及相关关键技术进行了分析和归纳。

课 后 练 习

一、填空题

1. 网络数据加密，通常分为链路加密、(　　　　　　)两种方式。
2. 防火墙的安全区域，通常分为外网、内网、DMZ 区三个区域，其中，DMZ 区又称为(　　　　　　)区。
3. 按工作原理划分，防火墙可分为(　　　　　　)和应用代理防火墙两大类。
4. 入侵检测系统的两种经典模型是(　　　　　　)和 CIDF。
5. 按照应用的方式划分，VPN 有两种基本类型：拨号 VPN 与(　　　　　　)VPN。

二、选择题

1. 端到端加密方式中，数据离开发送端后被最终的接收端收到之前，处于(　　)状态。

A. 加密　　B. 明文　　C. 加密或明文　　D. 不确定

2. 防火墙配置中的 ACL 指的是(　　)。

A. Access Content List　　B. All Content List

C. Access Condition List　　D. Access Control List

3. 包过滤防火墙的主要过滤依据是(　　)。

A. MAC 地址、端口、协议类型　　B. IP 地址、端口、协议类型

C. 域名、端口、协议类型　　D. IP 地址、域名、协议类型

4. 根据对收集到的信息进行识别和分析原理的不同，可以将入侵检测分为(　　)。

A. 异常检测、普通检测　　B. 滥用检测、普通检测

C. 异常检测、冲突检测　　D. 异常检测、滥用检测

5. 根据服务类型 VPN 业务分为(　　)VPN、Access VPN 与 Extranet VPN 三种。

A. Supernet　　B. Internet　　C. Intranet　　D. Subnet

三、简答题

1. 简述链路加密与端到端加密的主要特点。
2. 防火墙的主要功能局限性是什么？
3. 包过滤防火墙与应用代理防火墙的主要特点和应用场合是什么？
4. 按照入侵检测系统的检测对象划分，入侵检测系统分为哪几类？
5. 简述二层 VPN 和三层 VPN 的主要区别。

第12章　无线网络安全技术

随着相关技术的不断成熟和应用的普及，无线网络凭借其为用户提供的灵活性、便利性等优势，被迅速推广。现代企业随着业务规模的不断扩大和对工作效率提高的要求，越来越渴望灵活的无线网络技术能帮他们解决问题。此外，基于建设传统网络的繁琐和成本问题，很多用户也希望能通过无线网络技术实现他们灵活、迅速联网的目的。近几年，无线网络已经由时尚转变成为趋势。

本章重点

- 无线网络的分类及特点
- 移动通信网的安全特性及基本防护手段
- Wi-Fi 无线局域网的主要安全威胁、基本防护手段

12.1　无线网络安全概述

12.1.1　无线网络基础知识

无线网络是利用无线电波作为信息传输的媒介的网络，无线网络摆脱了网线的束缚。就应用层面来讲，它与有线网络的用途完全相似，两者的最大不同在于传输资料的媒介不同。除此之外，无线意味着无论是在网络硬件架设，还是网络的机动性、灵活性均比有线网络具备明显优势。无线网络目前主要分为 GSM/GPRS/CDMA/3G 无线上网、蓝牙和无线局域网(WLAN)几种类型。

无线网络的初步应用，可追溯到第二次世界大战期间，当时美国陆军采用无线电信号做资料的传输。他们研发出了一套无线电传输系统，并且采用高强度的加密算法，得到美军和盟军的广泛使用。他们也许没有想到，这项技术会在数十年后的今天改变我们的生活。1971年，夏威夷大学的研究员创造了第一个基于数据包传输的无线电通信网络。这个被称作 ALOHAnet 的网络，是世界上最早的无线局域网(WLAN)。它包括 7 台计算机，采用双向星状拓扑横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛上。从这时开始，无线网络正式诞生。

1990 年，IEEE 正式启动 802.11 项目，无线网络技术逐渐走向成熟。IEEE 802.11(Wi-Fi)标准诞生以来，先后有 802.11a、802.11b 和 802.11g 等标准被制定并应用，目前，为实现高宽度、高质量的无线网络服务，802.11n 也在被逐步推广。

2003 年以来，无线网络市场热度迅速飙升，目前已经成为 IT 市场中新的增长亮点。由于人们对网络速度及方便使用性的期望越来越大，于是与电脑以及移动设备结合紧密的 Wi-Fi、CDMA/GPRS、蓝牙等技术越来越受到人们的吹捧。与此同时，在配套产品大量面世之后，构建无线网络所需要的成本迅速下降，一时间，无线网络已经成为我们网络生活的主流。

12.1.2　无线网络技术

目前，主流的通过无线网络连入 Internet 的方式有两种。

第一种是通过移动电话卡(SIM 卡)，先连入移动电话运营商的网络(基站)，然后通过移动电话运营商的 Internet 网关连入 Internet。这种方式的优点是，只要有手机信号(移动公司、联通公司、电信的手机信号均可)的地方，均可连入 Internet，基本上做到了随时随地联网。但是这种方式目前的主要问题是，网络带宽相对还比较低，传输速度通常不高，且网络传输速度不稳定，受信号质量影响。

第二种是通过 WLAN(Wireless LAN，无线局域网)连入 Internet，Wi-Fi 是目前应用最广泛的无线局域网协议。这种方式要求某个场所已经通过特定方式连入了 Internet，然后在这个场所内发射无线信号，在无线信号范围覆盖内，根据设定的访问控制模式，任何支持 Wi-Fi 的设备，比如台式计算机、笔记本计算机、手机，乃至游戏机、MP3/MP4 播放器，均可连入 Internet。目前典型的具备 Wi-Fi 信号的场所有：机场、酒店、咖啡厅等公共场所，以及普通用户根据自己的需要，在办公场所或家里自行架设的无线局域网。这种无线上网的方式，通常上网带宽比较高，传输速度相对稳定，但上网受场所的制约，离开了相应的场所就无法上网，不能做到随时随地连入 Internet。

两种无线上网方式常常被混淆。比如，有的用户简单地理解为“无线上网就是使用手机上网”，这个理解显然是片面的。“手机上网”这个说法过于笼统，并没有把上网方式表达清楚。因为手机可以通过 SIM 卡和移动电话运营商通信来上网，也可用通过手机内置(也可通过其他接口连接)的 Wi-Fi 模块，连接附近的 Wi-Fi 局域网来上网。同样的道理，台式机、笔记本电脑或其他设备，都有两种上网方式选择。台式机连接 SIM 卡上网模块后，也可以连入移动电话运营商来连入 Internet，或者通过台式机所连接的 Wi-Fi 无线网卡连入附近的 Wi-Fi 局域网来上网。因此，我们在描述相关问题时，需要注意区分到底采用哪种上网方式，并对问题进行准确、清晰地表述。

下面我们来分别看看两种方式相关的技术。

1. GSM、CDMA 与 3G

目前，手机制式主要包括 GSM、CDMA、3G 三种，手机自问世至今，经历了第一代模拟制式手机(1G)、第二代 GSM、TDMA 等数字手机(2G)、第 2.5 代移动通信技术(CDMA)和第三代移动通信技术(3G)。

GSM 全名为 Global System for Mobile Communications，即全球移动通讯系统，俗称“全球通”。GSM 是一种起源于欧洲的移动通信技术标准，其开发目的是让全球各地可以共同使用一个移动电话网络标准，让用户使用一部手机就能通行全球。我国于 20 世纪 90 年代初引进并采用此项技术标准，此前一直是采用蜂窝模拟移动技术，即第一代 GSM 技术(2001 年

12 月 31 日我国关闭了模拟移动网络)。目前，中国移动、中国联通各拥有一个 GSM 网，为世界最大的移动通信网络。GSM 系统包括 GSM 900(900MHz)、GSM 1800(1800MHz)及 GSM 1900(1900MHz)等几个频段。

GSM 系统具有防复制能力强、网络容量大、手机号码资源丰富、通话清晰、稳定性强不易受干扰、信息灵敏、通话死角少、手机耗电量低等重要特点。

目前我国主要的两大 GSM 系统为 GSM 900 及 GSM 1800，由于采用了不同频率，因此适用的手机也不尽相同。不过目前大多数手机基本是双频手机，可以自由在这两个频段间切换。欧洲国家普遍采用的系统除 GSM 900 和 GSM 1800 另外加入了 GSM 1900，手机为三频手机。在我国随着手机市场的进一步发展，现也已出现了三频手机，即可在 GSM 900、GSM 1800、GSM1900 三种频段内自由切换的手机，真正做到了一部手机可以畅游全世界。

GSM 900 发展的时间较早，使用的较多，而 GSM 1800 发展的时间较晚。物理特性方面，前者频谱较低，波长较长，穿透力较差，但传送的距离较远，而手机发射功率较强，耗电量较大，因此待机时间较短。而后者的频谱较高，波长较短，穿透力佳，但传送的距离短，其手机的发射功率较小，待机时间则相应较长。

CDMA(Code Division Multiple Access)译为“码分多址分组数据传输技术”，被称为第 2.5 代移动通信技术。目前采用这一技术的市场主要在美国、日本、韩国等。CDMA 手机具有话音清晰、不易掉话、发射功率低和保密性强等特点，发射功率只有 GSM 手机发射功率的 1/60，被称为“绿色手机”。更为重要的是，基于宽带技术的 CDMA 使得移动通信中视频应用成为可能。

CDMA 技术的原理是基于扩频技术，即将需传送的具有一定信号带宽信息数据，用一个带宽远大于信号带宽的高速伪随机码进行调制，使原数据信号的带宽被扩展，再经载波调制后发送出去。接收端使用完全相同的伪随机码，与接收的带宽信号作相关处理，把宽带信号换成原信息数据的窄带信号(称为解扩)，以实现信息通信。

CDMA 的主要优点是：CDMA 中所提供的语音编码技术，可以把用户对话时周围环境的噪音降低，使通话更为清晰；CDMA 利用扩频的通讯技术，因而可以减少手机之间的干扰，并且可以增加用户的容量。而且手机的功率相对较低，不但可以使用时间增长，更重要的是可以降低电磁波辐射，在一定程度上减小对人的伤害；CDMA 的带宽可以进行较大的扩展，还可以传输影像；CDMA 具有良好的认证体制，更因为其传输的特性，大大地增强了防止被人盗听的能力。

3G 为英文 3rd Generation 的缩写，代表着第三代移动通信技术。手机自问世至今，经历了第一代模拟制式手机(1G)和第二代 GSM、TDMA 等数字手机(2G)，而当前通信运营商和终端产品制造商倡导的 3G 是指将无线通信与国际互联网等多媒体通信结合的新一代移动通信系统。它能够处理图像、语音、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务，为手机融入多媒体元素提供了强大的支持。

第三代通信网络的主要目标定位于实时视频、高速多媒体和移动 Internet 访问业务。早在 2000 年 5 月国际电信联盟(International Telecommunication Union，ITU)即确定了 W-CDMA、CDMA2000 和 TD-SCDMA 三个主流 3G 标准。

W-CDMA 即 Wide Band CDMA，意为宽频分码多重存取，是由 GSM 网发展出来的 3G 技术规范，其支持者主要是以 GSM 系统为主的欧洲厂商，包括欧美的爱立信、诺基亚、朗讯、北电以及日本的 NTT、富士通、夏普等厂商。这套系统能够架设在现有的 GSM 网络上，对于系统提供商而言可以较方便地过渡，而 GSM 系统相当普及的亚洲对这套新技术的接受度会比较高。因此，W-CDMA 具有先天的市场优势。目前 W-CDMA 手机已有多种产品面世，但国内还没有完善的 3G 网络可以应用。

CDMA2000 由美国高通公司为主导提出，摩托罗拉、朗讯和韩国三星都已参与，韩国现在成为该标准的主导者。这套标准是从窄频 CDMA2000 1X 数字标准衍生出来的，可以从原有的 CDMA2000 1X 结构直接升级到 CDMA2000 3X(3G)，建设成本低廉。但目前使用 CDMA 的地区主要只有日本、韩国和北美，中国联通正是应用了该模式过渡的，CDMA2000 的支持者不如 W-CDMA 多。不过 CDMA2000 的研发技术却是目前各标准中进度最快的，许多 3G 手机也已率先面世。

TD-SCDMA 全称 Time Division-Synchronous CDMA，该标准是由我国大唐电信公司提出的 3G 标准。该标准将智能无线、同步 CDMA 和软件无线电等当今国际领先技术融于其中。由于中国国内庞大的市场，该标准受到各大主要电信设备厂商的重视，全球一半以上的设备厂商都宣布可以支持 TD-SCDMA 标准。

2. WLAN

WLAN(Wireless LAN，无线局域网)就是在不采用传统网络线材的前提下，提供传统有线局域网的所有功能，网络所需的基础设施不用再埋在地下、管道中或隐藏在墙里，网络却能够随用户需要移动或变化。

无线局域网技术具有传统有线局域网无法比拟的灵活性。无线局域网的通信范围不受环境条件的限制，网络的传输范围大大拓宽，最大传输范围可达到几十公里。在有线局域网中，两个站点的距离在使用铜缆时被限制在 500 米以内，使用双绞线时则仅限于 100 米之内，即使采用单模光纤，若不对信号进行放大则传输距离也只能达到 3000 米，而无线局域网中两个站点间的距离目前可达到 50 公里，距离数公里的建筑物中的网络可以集成为同一个局域网。相对于有线网络，无线局域网的组建、配置和维护较为容易，一般计算机工作人员都可以胜任网络的管理工作。

无线局域网的主要标准有 Wi-Fi、蓝牙(Bluetooth)及 HomeRF(家庭网络)标准。典型的利用 Wi-Fi 组建的无线局域网如图 12-1 所示。

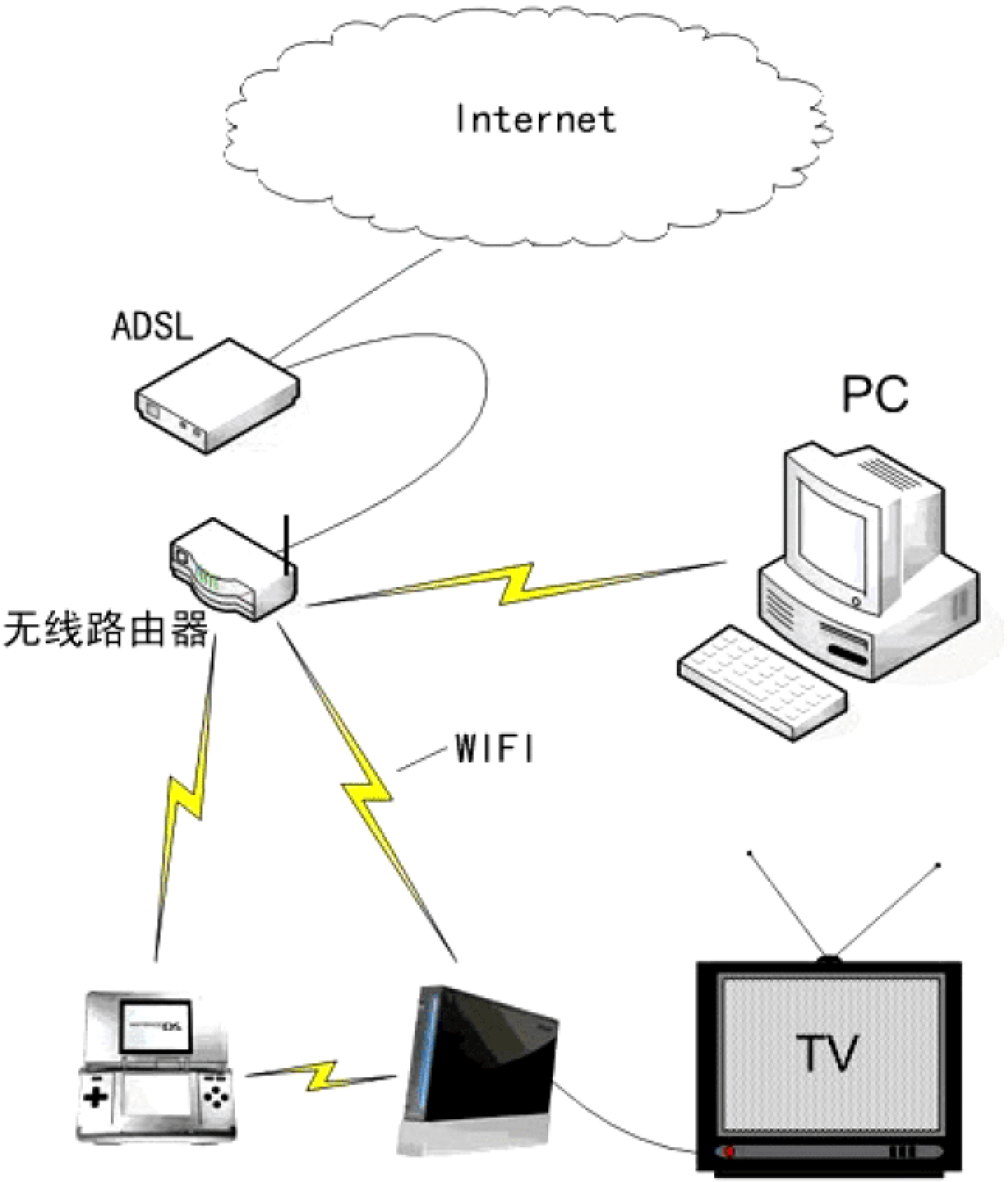


图 12-1　典型 Wi-Fi 无线局域网

Wi-Fi(Wireless-Fidelity，无线保真)是一个无线网络通信技术的品牌，由 Wi-Fi 联盟(Wi-Fi Alliance)所持有，用在基于 IEEE 802.11 标准的产品上，目的是改善基于 IEEE 802.11 标准的无线网络产品之间的互通性。Wi-Fi 联盟成立于 1999 年，当时的名称叫做 Wireless Ethernet Compatibility Alliance(WECA)。在 2002 年 10 月，正式改名为 Wi-Fi Alliance。普通用户通常会把 Wi-Fi 及 IEEE 802.11 混为一谈，甚至把 Wi-Fi 等同于无线局域网，事实上两者概念完全不同。IEEE 802.11 第一个版本发表于 1997 年，其中定义了媒体访问控制层(MAC)和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，数据传输速率设计为 2Mbit/s。两个设备之间的通信可以自由直接(Ad Hoc)方式进行，也可以在基站(Base Station，BS)或者访问点(Access Point，AP)的协调下进行。1999 年加上了两个补充版本：802.11a 定义了一个在 5GHz ISM 频段上的数据传输速率可达 54Mbit/s 的物理层，802.11b 定义了一个在 2.4GHz 的 ISM 频段上但数据传输速率高达 11Mbit/s 的物理层。2.4GHz 的 ISM 频段为世界上绝大多数国家通用，因此 802.11b 得到了最为广泛的应用。1999 年工业界成立了 Wi-Fi 联盟，致力解决符合 802.11 标准的产品的生产和设备兼容性问题。由此可知，Wi-Fi 为制定 802.11 无线网络的组织，而 IEEE 802.11 是一组网络协议。

蓝牙(IEEE 802.15)是一项新标准，对于 802.11 来说，它的出现不是为了竞争而是相互补充。“蓝牙”是一种先进的近距离无线数字通信的技术标准，其目标是实现最高数据传输速度 1Mbps(有效传输速率为 721Kbps)、传输距离为 10 厘米～10 米，通过增加发射功率可达到 100 米。IEEE 802.15 是由 IEEE 制定的一种蓝牙无线通信规范，应用于无线个人区域网(Wireless Personal Area Network，WPAN)。IEEE 802.15 具有许多特征，如短程、低能量、低成本、小型网络及通信设备，适用于个人操作空间。

HomeRF 主要为家庭网络设计，是 IEEE 802.11 与 DECT(数字无绳电话)标准的结合，目

的在于降低语音数据成本。HomeRF 采用了扩频技术，工作在 2.4GHz 频段，能同步支持 4 条高质量语音信道。随着 Wi-Fi 的迅速发展，HomeRF 已经逐渐退出市场。

目前，有线接入技术主要包括以太网、xDSL 等。Wi-Fi 技术作为高速有线接入技术的补充，具有为可移动性、价格低廉的优点，Wi-Fi 技术广泛应用于有线接入需无线延伸的领域，如临时会场等。由于数据速率、覆盖范围和可靠性的差异，Wi-Fi 技术在宽带应用上将作为高速有线接入技术的补充。而关键技术无疑决定着 Wi-Fi 的补充力度。现在 OFDM、MIMO(多入多出)、智能天线和软件无线电等，都开始应用到无线局域网中以提升 Wi-Fi 性能，如 802.11n 计划采用 MIMO 与 OFDM 相结合，使数据速率成倍提高。另外，天线及传输技术的改进使得无线局域网的传输距离大大增加，可以达到几公里。

12.2　无线网络安全性分析

12.2.1　移动通信网络安全性分析

基于无线网络的特点，在方便合法用户接入网络的同时，也使得无线网络更容易被非法用户攻击。移动通信网络面临的用户数量大，且多数用户不具备基本的网络技术知识以及安全防范意识，因而移动通信网络的安全问题相对更加复杂。

1. GSM 网络安全

GSM 网络安全性体现在三个方面：用户身份的保密性、认证和加密。通过认证，防止没有授权的用户使用网络资源；通过加密，保证用户数据和信令数据的保密性。具体内容如下。

采用临时号码(TMSI)来保证用户身份的保密性。GSM 系统为每个移动用户分配一个唯一的国际移动用户识别码(International Mobile Subscriber Identifier，IMSI)。它存储于 SIM 卡的 EPROM 中，这个身份一旦被非法用户利用就可能对用户和移动运营商带来损失。GSM 系统中通过采用 TMSI 实现用户身份的保密性。TMSI 只有临时和局部的作用，经过一段时间或跨越不同的区域时，TMSI 都会进行更新，更新的频率由移动运营商自行设置。在更新时，TMSI 的传输采取加密方式。为了避免混淆，所以要和位置标识符(Location Area Identity，LAI)一起使用。IMSI 只有在当接收到 TMSI 与 LAI 不匹配时才需要发送，通常在用户接入网络时才使用。这样，如果跟踪用户就只能跟踪到临时号码 TMSI，而没办法查出用户的真实用户识别码 IMSI。

GSM 系统中的用户身份认证，采用 Challenge Response 机制(查问/应答鉴别机制)的一系列密钥认证系统来实现。在移动终端、网络交换子系统中同时保存密钥 Ki 用于实现认证，它存在于认证中心和 SIM 卡中。其具体步骤如下：首先，移动终端的随机数产生器生成一个长度为 128 位的随机数，该数被送到移动终端中；然后，网络子系统的认证中心和移动终端利用 Ki 和产生的随机数通过 A3 算法分别得出一个带符号的结果(SRES)。并将移动终端所产生的 SRES 发送到认证中心；最后，对两个得出的结果(SRES)进行比较，如果结果不同，则拒绝接入的请求。由于 GSM 系统在每次用户接入时进行身份认证，每次产生的随机数是不一

样的，所以尽管上次可能在无线通道上被窃听到有关身份认证的消息，下一次随机数发生改变，也无法利用。

GSM 的数据在无线信道上采用加密传输的方式，使用户信息和信令信息不容易被窃听，以实现用户信息和信令信息的保密性。用户身份认证通过后，移动终端就由 Ki 和所产生的随机数作为输入，通过 A8 算法产生加密密钥 Kc，并将此加秘密钥送到所访问的 VLR(Visitor Location Register，访客位置寄存器)中。Kc 和帧号码用于 A5 算法，以对移动终端与访问系统之间的数据流进行加密和解密。

2. 3G 网络安全

用户可利用移动终端随时接入 Internet，因而 3G 网络面临着与 Internet 同样复杂的安全问题。3G 网络中的安全技术是在 GSM 的安全机制基础上建立起来的，它克服了 GSM 中的一些安全问题，并增加了新的安全功能，为用户和移动服务提供商提供更为可靠的安全机制。3G 系统融合了无线通信与 Internet 技术，3G 的安全将更多地使用 Internet 中各种成熟的加密技术。根据 3GPP(3rd Generation Partnership Project，第三代合作伙伴计划)和 WAP(Wireless Application Protocol，无线应用协议)的标准化规定，3G 中运用了许多新的及增强型的安全技术，具体内容如下。

1) 入网安全

用户信息通过开放的无线信道进行传输，因而很容易受到攻击。第二代移动通信系统的安全标准主要关注的也是移动终端到网络的无线接入的安全性。在 3G 系统中，提供了相对于 GSM 而言更强的安全接入控制，同时考虑了与 GSM 的兼容性，使得 GSM 平滑地向 3G 过渡。与 GSM 中一样，3G 中用户端接入网安全也是基于一个物理和逻辑上均独立的智能卡设备，即 USIM。未来的接入网安全技术将主要关注如何支持在各异种接入媒体包括蜂窝网、无线局域网以及固定网之间的全球无缝漫游，这将是一个全新的研究领域。

2) 核心网安全技术

与第二代移动通信系统一样，3GPP 组织最初也并未定义核心网安全技术。但是随着技术的不断发展，核心网安全也已受到了人们的广泛关注，在可以预见的未来，它必将被列入 3GPP 的标准化规定。目前一个明显的趋势是，3G 核心网将向全 IP 网过渡，因而它必然要面对 IP 网所固有的一系列问题。Internet 安全技术也将在 3G 网中发挥越来越重要的作用，移动无线因特网论坛(Mobile Wireless Internet Forum，MWIF)正致力于为 3GPP 定义一个统一的结构。

3) 传输层安全

尽管现在已经采取了各种各样的安全措施来抵抗网络层的攻击，但是随着 WAP 和 Internet 业务的广泛使用，传输层的安全也越来越受到人们的重视。这一领域的相关协议包括 WAP 论坛的无线传输层安全(WTLS)、IEFT 定义的传输层安全(TLS)、之前定义的 Socket 层安全(SSL)。这些技术主要是采用公钥加密方法，利用 PKI 技术进行相关数字签名及认证，为需要在传输层建立安全通信的实体提供安全保障。

4) 应用层安全

在 3G 系统中，除提供传统的话音业务外，电子商务、电子贸易、网络服务等新型业务

将成为 3G 的重要业务发展点。因而 3G 将更多地考虑在应用层提供安全保护机制。端到端的安全以及数字签名可以利用标准化 SIM 应用工具包来实现，在 SIM/USIM 和网络 SIM 应用工具提供商之间建立一条安全的通道。SIM 应用工具包安全定义参见 3GPP GSM TS 03.48。

5) 代码安全

第二代移动通信系统中，所能提供的服务都是固定的、标准化的，但是在 3G 系统中各种服务可以通过系统定义的标准化工具包来定制(例如 3GPP TS 23.057 定义的 MExE)。MExE 提供了一系列标准化工具包，支持用手机终端进行新业务和新功能下载。这一过程中，虽然考虑了一定的安全保护机制，但相对有限。MExE 的使用增强了终端的灵活性，但也使得恶意攻击者可以利用伪“移动代码”或病毒对移动终端软件进行破坏。

12.2.2　Wi-Fi 无线局域网安全性分析

Wi-Fi 无线局域网所采用的 IEEE 802.11 标准最早于 1999 年发布，它描述了无线局域网(Wireless Local Area Network，WLAN)和无线城域网(Wireless Metropolitan Area Network，WMAN)的媒体访问控制(链路层)和物理层的规范。为了防止出现无线局域网数据被窃听，并提供与有线网络中功能等效的安全措施，IEEE 引入了有线等价保密(Wired Equivalent Privacy，WEP)算法。和许多新技术一样，最初设计的 WEP 被人们发现了许多严重的弱点。专家们利用已经发现的弱点，攻破了 WEP 声称具有的所有安全控制功能。对普通用户来说，利用网上下载的工具，可以轻松破解基于 WEP 加密的 Wi-Fi 无线网。总的来说，WEP 存在如下弱点。

- 整体设计问题。在无线网络环境中，不使用保密措施是具有很大风险的，但 WEP 协议只是 802.11 设备实现的一个可选项。
- 加密算法问题。WEP 中的初始化向量(Initialization Vector，IV)由于位数太短和初始化复位设计，容易出现重用现象，从而导致密钥被破解。WEP 用于进行流加密的 RC4 算法，在其头 256 个字节数据中的密钥存在缺陷，目前尚无有效的修补办法。此外用于对明文进行完整性校验的循环冗余校验(Cyclic Redundancy Check，CRC)算法，只能确保数据被正确传输，并不能保证其未被修改，因而不是安全的校验码。
- 密钥管理问题。802.11 标准要求 WEP 使用的密钥需要接受一个外部密钥管理系统的控制。通过外部控制可以减少 IV 的冲突数量，使得无线网络难以攻破。但问题在于这个过程形式非常复杂，并且需要手工操作，因而很多网络的部署者更倾向于使用缺省的 WEP 密钥，这使黑客为破解密钥所作的工作量大大减少。另一些高级的解决方案需要使用额外资源，如 Radius 和 Cisco 的 LEAP 协议，成本比较昂贵。
- 用户行为问题。许多用户都不会修改缺省的配置选项，使得黑客很容易推断出或猜出密钥。

未采用 WEP 加密的 Wi-Fi 无线网安全性比 WEP 有明显改善，也并非高枕无忧，主要有以下几种隐患。

- 无线网络非常容易被发现。为了能够使合法用户找到无线网络，网络必须发送含有特定参数的数据帧，这样就给攻击者提供了必要的网络信息。入侵者可以通过高灵

敏度天线从公路边、楼宇中以及其他任何地方对网络发起攻击，而不需要任何物理方式的侵入。

- 未经授权访问无线网络。相当一部分普通用户在使用无线接入设备(如无线路由器)时，只在其默认的配置基础上进行很少的修改，此时这些无线接入设备都按照默认配置来开启 WEP 进行加密，或者使用原厂提供的默认密钥。由于无线局域网的开放式访问方式，未经授权使用网络资源不仅会增加带宽费用，更可能会导致法律纠纷。而且未经授权的用户没有遵守服务提供商提出的服务条款，可能会导致 ISP 中断服务。
- 地址欺骗和会话拦截。由于 802.11 无线局域网对数据帧不进行认证操作，攻击者可以通过欺骗帧来重定向数据流，使 ARP 表变得混乱。通过非常简单的方法，攻击者可以轻易获得网络中站点的 MAC 地址，这些地址可以被用于恶意攻击。除攻击者通过欺骗帧进行攻击外，攻击者还可以通过截获会话帧发现无线接入设备中存在的认证缺陷，通过监测无线广播帧确认无线接入设备的存在。攻击者很容易装扮成无线接入设备进入网络。
- 流量分析与流量侦听。802.11 无法防止攻击者采用被动方式监听网络流量，而任何无线网络分析仪都可以不受任何阻碍地截获未进行加密的网络流量。

12.3　无线网络安全防护

12.3.1　移动通信网络安全防护

随着移动通信系统在各行业的广泛应用，对移动通信安全也提出了更高的要求。未来的移动通信系统安全需要进一步的加强和完善，具体表现在以下几个方面。

1. 3G 的安全体系结构趋于透明化

目前的 3G 网络安全体系仍然建立在假定内部网络绝对安全的前提下，但随着通信网络的不断发展，终端在不同运营商乃至异种网络之间的漫游也成为可能，因此应增加核心网之间的安全认证机制。特别是随着移动电子商务的广泛应用，更应尽量减少或避免网络内部人员的干预性。未来的安全中心应能独立于系统设备，具有开放的接口，能独立地完成双向鉴权、端到端数据加密等安全功能，甚至对网络内部人员也是透明的。

2. 考虑采用公钥密码体制

在希望未来的 3G 网络更具有可扩展性，安全特性更加具有可见性、可操作性的趋势下，采用公钥密码体制。参与交换的是公开密钥，因而增加了私钥的安全性，并能同时满足数字加密和数字签名的需要，满足电子商务所要求的身份鉴别和数据的保密性、完整性、不可否认性。因此，必须尽快建设无线公钥基础设施(WPKI)，建设以认证中心(CA)为核心的安全认证体系。

3. 考虑新密码技术的应用

随着密码学的发展以及移动终端处理能力的提高，新的密码技术，如量子密码技术、椭圆曲线密码技术、生物识别技术等已在移动通信系统中获得广泛应用，加密算法和认证算法自身的抗攻击能力更强，从而保证传输信息的保密性、完整性、可用性、可控性和不可否认性。

4. 使用多层次、多技术的安全保护机制

为了保证移动通信系统的安全，不能仅依靠网络接入和核心网内部的安全机制，而应该使用多层次、多技术相结合的保护机制。在应用层、网络层、传输层和物理层上进行全方位的数据保护，并结合多种安全协议，从而保证信息的安全。

今后相当长一段时期内，移动通信系统都会出现 2G 和 3G 两种网络共存的局面，移动通信系统的安全也面临着后向兼容的问题。因此，如何进一步完善移动通信系统的安全，提高安全机制的效率以及对安全机制进行有效的管理，都是亟需解决的问题。

12.3.2　Wi-Fi 无线局域网安全防护

针对 Wi-Fi 无线局域网的安全防护，主要有以下几种措施。

1. 加强网络访问控制

通过强大的网络访问控制可以减少无线网络配置的风险。如果将无线接入设备安置在像防火墙这样的网络安全设备之外，应考虑将其通过 VPN 技术连接到主干网络，更好的办法是使用基于 IEEE 802.1x 协议的无线网络产品。IEEE 802.1x 定义了新的用户级认证的数据帧类型，借助于企业网已经存在的用户数据库，将前端基于 IEEE 802.1X 无线网络的认证转换到后端基于有线网络的 Radius 认证。

2. 加强安全认证

加强安全认证的最好防御方法就是阻止未被认证的用户进入网络，由于访问权限控制是基于用户身份的，所以通过对认证过程进行加密是进行认证的前提，通过 VPN 技术能够有效地保护通过无线电波传输的网络流量。一旦配置好无线网络，严格的认证方式和认证策略将是至关重要的。另外还需要定期对无线网络进行测试，以确保网络设备使用了安全认证机制，并确保网络设备的配置正常。需要强调的是，应杜绝使用 WEP 加密方式，而采用 WPK(Wi-Fi Protected Access)协议加密，并设置 8 位以上的密码。

图 12-2 所示是一个常见的无线路由器的配置界面。其中，Security Mode(安全模式)选项有 WEP、Radius、WPA、WPA2、WPA2 Personal 等，因 WEP 的安全性太差，本例选择的是 WPA2 Personal 模式。WPA Algorithms(WPA 加密算法)选择的 TKIP＋AES，是比较安全的一种算法。WPA Shared Key(WPA 共享密钥)，设置了一个比较长的密钥。因此，图 12-2 所示是相对比较安全的一种设置，是对无线接入设备进行设置的基本要求。

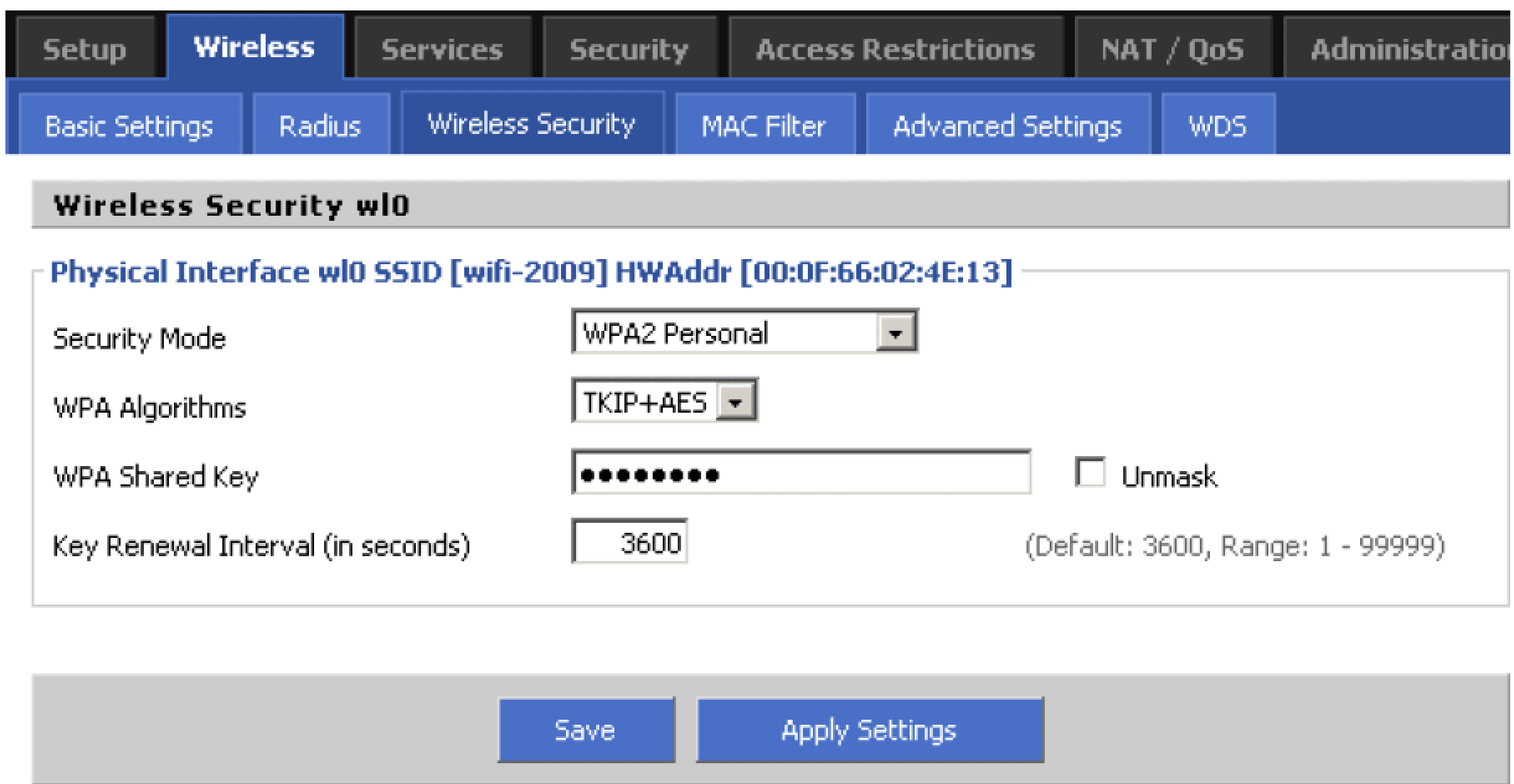


图 12-2　无线接入设备的基本安全设置

3. 重要网络隔离

在支持新的安全机制的无线网络协议应用之前，MAC 地址欺骗对无线网络的威胁依然存在。网络管理员必须将无线网络同易受攻击的核心网络进行物理隔离，两类网络间不允许任何形式的连接。

4. 合理配置、安装无线接入设备

对于自己搭建无线网络的用户，需要进行一些最基本的安全配置，如隐藏 SSID，关闭 DHCP，设置 WPA 密钥，启用内部隔离等。条件允许的用户，应配置 MAC 过滤，建立 802.1x 端口认证。此外，在安装无线接入设备时，可使用定向天线，调整发射功率，尽可能把信号收敛在信任的范围之内。还可以将无线局域网视为 Internet 一样来防御，甚至在接口处部署入侵检测系统。

本 章 小 结

本章介绍了两大类无线网络的简要发展历程，阐述了无线网络带来巨大的网络部署效率、灵活性提升，并分析了由此带来的巨大安全隐患。特别是当前广泛普及的 Wi-Fi 无线局域网。针对两类无线网络的安全防护，是已经或将要连入无线网络的用户需要引起足够重视的问题，只有安全的连入无线网络，才能真正提高工作效率，否则因安全问题带来的影响将会得不偿失。

课 后 练 习

一、填空题

1. 1971 年，夏威夷大学研究员创造的第一个无线通信网络，被称为(　　　　　　)。

2. 当前主要有两种无线接入 Internet 的方式，即通过移动通信网络接入和通过(　　　　　　)接入。

3. GSM 安全性体现在用户身份的保密性、认证和(　　　　　　)三个方面。

4. Wi-Fi 采用的是 IEEE (　　　　　　)系列协议。

5. Wi-Fi 的加密方式主要有 WEP、WPA 两种，其中，(　　　　　　)的安全性比较差，很容易被破解。

二、选择题

1. 蓝牙属于(　　)。

A. 有线局域网　　B. 无线局域网　　C. 移动通信网　　D. 以上都不是

2. 蓝牙采用的网络协议是(　　)。

A. IEEE 802.3　　B. IEEE 802.11

C. IEEE 802.15　　D. IEEE 802.16

3. 传输层安全机制 SSL 的缩写来自于(　　)。

A. Safe Sockets Layer　　B. Safe Signal Layer

C. Secure Sockets Layer　　D. Secure Signal Layer

4. IEFT 定义的传输层安全机制是(　　)。

A.TCP　　B. UDP　　C. HTTPS　　D. TLS

5. 加强 Wi-Fi 安全性的措施之一是(　　)。

A. 隐藏 SSID　　B. 显示 SSID

C. 不设置 SSID　　D. 以上都不是

三、简答题

1. 与有线网络相比，无线网络的主要优势是什么？
2. 与有线网络相比，无线网络的主要不足是什么？
3. Wi-Fi 和蓝牙的各自优点、缺点及适用场合是什么？
4. 为何采用 WEP 加密机制的 Wi-Fi 无线网络密码很容易被破解？
5. 3G 无线上网与 Wi-Fi 无线上网各自的优缺点是什么？

第13章　网络应用安全

Internet是一个庞大、复杂的系统，其运行过程中任何一个环节都需要安全保障。网络应用安全符合典型的“木桶原理”，任何一个环节出现问题，整个应用系统的安全性就会遭到破坏。网络应用的存取控制，应用数据在网络中传输的各个环节，以及各类丰富的Web应用系统，都面临着错综复杂的风险，层出不穷的攻击手段使得网络应用安全形势日趋严峻。

本章重点

- 网络攻击的主要步骤
- 设置安全口令的基本准则
- 网络监听的基本原理与防范
- 网络扫描的概念、防护手段
- 网络钓鱼的概念及其防范
- SQL注入及基本防护

13.1　网络攻击的步骤

通过学习第8章内容可知，在一次完整的入侵过程中，第一步就是要获取对目标系统的远程控制权。在实施这一步之前，必须进行充足的准备工作，这样才能提高入侵的成功率。盲目的攻击不仅难以收到成效，更容易暴露自己，带来麻烦。这里所说的准备工作，就是攻击前的信息搜集，俗称“踩点”，好比略有水平的罪犯，在犯罪前必定要先勘测现场。

卓有成效的信息搜集过程应包含以下几个步骤。

13.1.1　搜集初始信息

确定攻击目标后，需要先搜集初始信息，如IP地址或域名。然后攻击者可根据已知的域名查找关于这个站点的信息。比如站点服务器的存放地理位置或维护站点的工作人员，这些都能够帮助攻击者了解被攻击对象。搜集初始信息的方法包括以下几种。

1. 开放来源信息

很多时候，目标站点发布的公共内容，会在不知不觉中泄露大量信息，因而被攻击者利用。这种信息通常被称为开放来源信息。

开放的来源是指关于攻击目标或者它的合作伙伴的一般、公开的信息，任何人能够得到。这意味着存取或者分析这种信息比较容易，且获取这些信息时不会被怀疑。这里列出几种获取开放来源信息的例子：目标主机的新闻信息，如某公司为展示其技术的先进性和能为客户提供最好的监控能力、容错能力、服务速度，往往会不经意间泄露了系统的操作平台、交换机型号及基本的线路连接情况；目标主机的员工信息(大多数公司网站上附有姓名地址簿，这些都能提供了一些有用的信息)。

2. Whois

对于攻击者而言，任何有域名的公司必定泄露某些信息。攻击者对目标域名执行 Whois 查询，即可找到目标相关信息。通过查看 Whois 的输出，攻击者会得到一些非常有用的信息，例如得到一个物理地址、一些人名和电话号码(可用于社会工程学攻击)。通过 Whois 查询还可获得目标域名的主、从服务器 IP 地址。

3. Nslookup

Nslookup(Name System Lookup)即域名系统查询是用于查询目标域名内的各类DNS 记录的命令行工具，也是查找目标主机其他 IP 地址的方法之一。DNS 查询结果还包括目标域内的 MX 记录，从而了解目标域内的邮件服务器信息。一般用户的做法都是将服务器放在同一 IP 地址段中，通过 DNS 查询，还可猜测出攻击目标临近的服务器 IP。

获得攻击目标 IP 地址的更简单的方法是使用 ping 命令，参数是目标域名。ping 一个域名时，TCP/IP 协议栈首先要将目的域名解析为 IP 地址，并在屏幕上显示目的 IP。

13.1.2　确定攻击目标的 IP 地址范围

当攻击者明确单个目标主机的 IP 地址后，通常还要找出网络的 IP 地址范围及子网掩码。这样做有两方面的原因：其一，假设有目的 IP 地址为 10.10.10.5，要扫描整个 A 类地址段需要相当长的时间。如果确定目标只是该 A 类地址段的一个很小的子集，则能大大节省扫描时间，加快攻击进度。其二，某些攻击目标安全防范措施较好，对其进行扫描会触发报警，因而扫描大的地址段风险较大。

达到此目的的主要手段是使用 traceroute 命令，该命令可以知道一个数据包在通过网络时的各段路径。利用这一信息，能判断主机是否在相同的网络上。通常，连入 Internet 上的网络都会设置一个出口路由器(或类似设备)，并通过防火墙后的交换机连接其他入网计算机。因此 traceroute 输出的最后一跳(Hop，指最后一个节点)是目的机器，倒数第二跳是防火墙，倒数第三跳则为出口路由器。通过同一出口路由器的所有计算机都属于同一网络。因此攻击者查看通过 tranceroute 到达的各种 IP 地址，根据这些目的 IP 是否通过相同的出口路由器，就能初步判断它们是否属于同一网络。

13.1.3　扫描存活主机、开放的端口

确定目标 IP 地址范围后，攻击者需要了解目标网络中有哪些存活主机。目标网络中不同段会有不同的主机处于开机状态。通常攻击者在白天扫描活动的机器，然后深夜再次查找，

这样能大致区分个人计算机和服务器，因为服务器始终都处于运行状态，而个人计算机通常只在白天开机。

ping 命令是用来测试目标主机的存活状态的基本方法。如果目标主机上安装了防火墙，并设置不响应 ping 命令发出的连通性测试数据包，则需要使用其他办法来判断目标主机是否在网络中。为了提高扫描效率，通常使用专用的扫描工具软件来进行扫描，并且这类工具会提供类似 ping 命令等多种方式来对设定的 IP 地址段进行扫描。

针对目标网络中的存活主机，需要进一步了解其运行状况。首先要掌握的就是目标主机上开放了哪些端口。根据开放的端口来判断是否有相应的漏洞可利用，或根据端口上开放的服务来分析目标系统的运行状况。

端口扫描和存活主机扫描通常在一次扫描过程中完成。

13.1.4　分析目标系统

根据存活主机扫描、端口扫描过程中目标主机返回的信息，能在某种程度上判断目标主机使用的是哪一种操作系统。不同的操作系统有不同的漏洞，相应有着不同的漏洞利用程序及入侵步骤。

此外，分析目标主机的开放端口上监听的服务，能获得关于目标的更多信息。例如，扫描得知目标主机的 TCP 25 端口处于开放状态，则可连接到该端口，了解目标主机上运行的电子邮件服务程序的名称、版本号，然后查找相应邮件服务程序对应的版本是否有可利用的漏洞。

有一些探测远程主机并确定在运行哪种操作系统的程序。这些程序通过向远程主机发送不平常的或者没有意义的数据包来完成。因为这些数据包 RFC(internet 标准)没有列出，一个操作系统对它们的处理方法不同，攻击者通过解析输出，能够弄清自己正在访问的是什么类型的设备和在运行哪种操作系统。

总之，对目标系统了解越多，找到其缺陷、漏洞的可能性也就越大。

13.2　口 令 安 全

对网络应用和非网络应用来说，口令机制是最基本的保护措施。

对非网络应用而言，如有敏感数据希望不被他人查看，可采用加密压缩(打包)进行存放，或者使用专用的基于文件或基于磁盘分区的加密工具软件保存数据，这样能在很大程度上保障数据的安全。但是，数据加密对数据的保护效果和操作者的使用方式、使用习惯有很大的关系。例如，对 Word 文档的保护，使用 Word 自身提供的口令机制，其受保护程度是非常脆弱的，因为 Office 2003 及之前的版本均存在使用 RC4 加密算法时的漏洞，即使是长达 20 多个字符的口令，通过漏洞利用工具，也可在几秒钟的时间内破解。

基于用户名、口令的访问控制机制，是网络应用的基本安全防范机制。许多网络应用会涉及经济活动或经济利益，由此也出现了大量用于盗取网络应用口令的密码窃取工具。各类网络应用为了降低密码被盗的概率，绞尽脑汁采取了各种手段，将用户输入用户名、口令的

过程以尽可能安全的方式进行保护。

13.2.1　口令破解

典型的口令破解有以下几种方法。

1. 暴力破解

就是利用程序自动排列字符和数字的组合，并利用这个排列尝试登录系统的过程。从理论上来说，这种方式能破解任何系统的口令，但实际中这种方式往往是效率最低的，在系统有基本的防范措施的情况下，依靠暴力破解的方式是不可能获得成效的。对于简单口令来说，暴力破解的破坏力是相当强大的。如果口令位数不多，对于现代计算机的计算能力来说，破解就是几秒钟的事情。

2. 字典破解

将一些网络用户经常、习惯使用的口令，以及曾经通过各种手段所获取的其他系统的口令，集中在一个文本文件中。破解程序读取这个“字典”文件，针对目标系统自动逐一进行测试登录。也就是说，只有当目标用户的口令存在于其字典文件中，才会被这种方式找到。这个看上去“守株待兔”的方法的实际效果往往好于预期。由于网络上经常有不同的黑客彼此交换字典文件，因此一份网上流传的字典文件，通常是包含了很多黑客对于口令经验的积累。对于安全意识不高的用户，这种方式的破解成功率较高。

3. 掩码破解

所谓掩码口令是假设我们已经知道口令的某一位或几位，此时可以对该位设置掩码，将口令的其他各位使用字符、数字的各种组合，通过不断尝试来猜测口令。由于已经确定口令中部分位置的字符，因而在此前提下破解效率能得到一定提高。这种破解方式常常和社会工程学结合，因为许多用户习惯用生日、门牌号码、电话号码等日常生活中用到的数字做密码，在口令猜测过程中利用相关目标的这些信息，能显著提高破解成功率。

4. 网络嗅探破解

与前 3 种方式相比，这种方式不同之处在于并非通过不断的尝试来破解口令。这种方式的工作原理是，通过捕获网络上流过的数据，从中找出相关的口令。图 13-1 是一次 Web 邮箱登录过程中捕获到的网络数据，登录的是 Internet 上的免费邮件系统 http://mail.yeah.net/，读者可用协议分析软件自行做类似的实验。注意观察图 13-1 中方框中的数据“cookie=&user=test2007&pass=qwerzxcv123”，即可看到该邮箱用户的用户名为“test2007”，口令为“qwerzxcv123”。这种口令破解方式在相关应用系统缺乏基本的防范措施时非常有效。显然，一个专业的应用网络应用系统，不应该将用户账号信息以明文的方式在网络中传输。

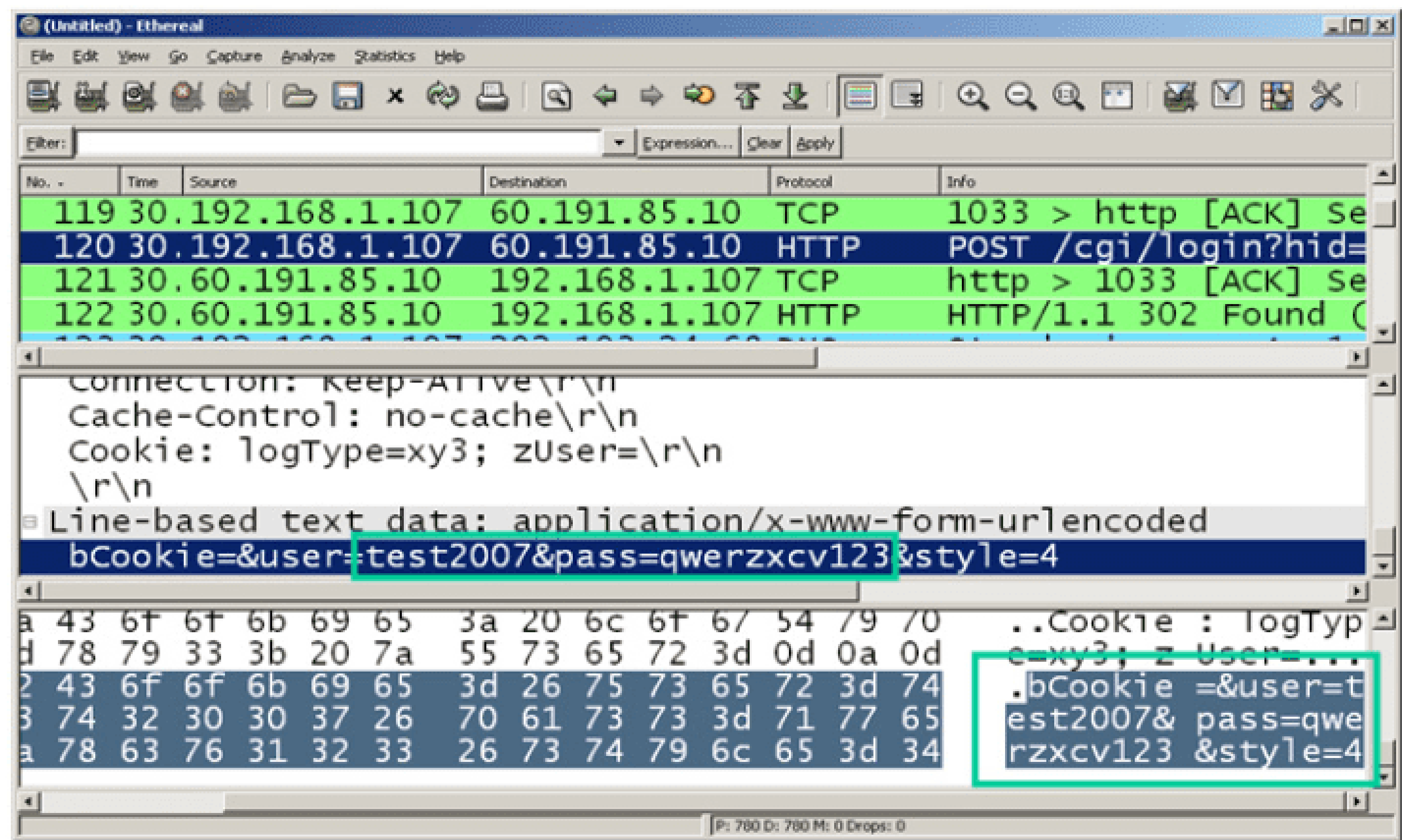


图 13-1　利用捕获到的网络数据包

13.2.2　设置安全的口令

使用与个人、亲人、朋友的信息相关的数字作为口令是典型的“弱口令”，这种口令极易被破解。口令越长、越复杂越安全，例如，好的口令不应仅仅包含数字或仅仅包含字符，甚至字符也不应仅仅包含小写或仅仅包含大写。如果再结合“%#!$^_+”等字符，这个口令就更安全了。

然而，较长较复杂的口令安全性是足够了，易用性却太差。因而好的口令应当不仅仅指口令够复杂、够长。好的口令应当是指其构造方法：口令容易记住，但很难被破解。以下是设置好的口令的一套准则。

1. 选择核心短语

开始要选一个至少 5 个单字长的短语。这可以是某首歌的头一行、一句引语或者是书名，或者是一段汉字的拼音，只要能牢记就行。然后利用该短语创建核心口令，通常的办法是取每个单词的头一个字母。

比如 esotsm，这是电影《Eternal Sunshine of the Spotless Mind》的头一个字母组成的口令。

这个简单的步骤可以保护口令免遭受字典破解攻击。因为字典里面的每个条目通常是由完整的单词组成的。

2. 用大写字母、数字或者符号替代一些小写字母

注意混合使用大写、小写字母及数字，在脑子里记住替换规则，这样无需将替换后的口令写在纸上或文件中，从而避免被发现。

例如前面的口令 esotsm，我们将第一个和最后一个字符替换为大写，将其中的字符“o”替换为数字“0”，则替换之后口令变为 Es0tsM。

这个步骤显著提高了口令的复杂性，替换前只需排列组合所有的小写字符，替换后则需排列组合所有的大写字符、小写字符、数字，使得暴力破解的可能性大大降低。

3. 针对各个主机或应用定制口令

例如，使用同一个核心口令，在此基础上根据不同应用再添加若干与主机或应用系统相关、便于记忆的字符。

例如，基于前述核心口令 Es0tsM，我们可以把 ThinkPad X60 笔记本上的操作系统口令设置为 Es0tsMTPX60，把运行邮件服务器的 HP 380G5 服务器的操作系统口令设置为 Es0tsMHP380G5。口令长度加长了，但记忆难度却基本不变。

4. 根据不同安全需求等级设置不同的口令

如果相关账户不涉及财务信息，则通常使用一个核心口令短语即可。但如果账户用于信用卡号码、涉密信息等，就必须使用不同的核心短语，为安全起见，还应组合两三个核心短语，从而加强口令的安全性。

理想情况下，应当至少每隔 90 天就要更改口令。然而实际操作中，因管理机制、人员素质等原因，口令及时更换的操作常常未能有效实施。

13.3 网 络 监 听

网络监听，又称为网络嗅探(Sniff)，是指利用工具软件或专用硬件，将网络中某节点流经的数据包捕获下来，进行分析或用作其他用途。实现网络监听的工具软件，称为 Sniffer。典型的网络监听工具软件有 Ethereal(开源软件，后更名为 WireShark)、WildPacket EtherPeek(新版本更名为 WildPacket OmniPeek)、Sniffer Pro 等。本书中的例子以开源软件 Ethereal 为主来介绍。

网络监听技术通常是提供给网络安全管理人员进行管理的工具，可以用来监视网络的状态、数据流动情况以及网络上传输的信息等。当信息以明文的形式在网络上传输时，使用监听技术进行攻击很容易，只要将网络适配器(即网卡)设置成监听模式(又称混杂模式)，便可以源源不断地截获网上传输的信息。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。

13.3.1 网络监听原理

目前，局域网市场中，占绝对统治地位的以太网使用的 CSMA/CD(Carrier Sense Multiple Access with Collision Detection，带冲突检测的载波监听多路访问)，其工作方式是：将要发送的数据帧发往连接在一起的所有主机，帧中包含着目的主机的网卡地址(MAC 地址)，只有与数据帧中地址一致的那台主机才会接收此帧，其他主机收到后直接丢弃此帧。但是，若主机的网络接口工作监听模式下，则无论数据帧中的目标地址是多少，主机都会接收此帧(当然只能监听经过自己网络接口的那些包)。

在 Internet 上有很多使用以太网协议的局域网，许多主机通过电缆、集线器、交换机连在一起。当同一网络中的两台主机通信时，源主机将写有目的主机 IP 地址的数据包直接发向目的主机 IP。但这种数据包不能在 IP 层直接发送，必须把 TCP/IP 协议的网络层交给下层协议，即链路层，而网络接口是不识别 IP 地址的，因此在网络层的数据包向下到链路层时，会增加一个以太网的帧头的信息。在帧头中有两个域，分别为只有网络接口才能识别的源主机和目的主机的物理地址，即 MAC 地址。

传输数据时，包含物理地址的帧从网络接口(网卡)发送到物理线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，能够到达线路上的每一台主机。当使用集线器时，由集线器再发向连接在集线器上的每一条线路，数字信号也能到达连接在集线器上的每一台主机。当数字信号到达一台主机的网络接口时，正常情况下，网络接口读入数据帧进行检查，如果数据帧中携带的物理地址与自己的地址匹配，数据帧中的物理地址是广播地址，则将数据帧交给上层协议软件，也就是网络层协议软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都进行这个处理过程。

然而，当主机工作在监听模式下，所有的数据帧都将被交给上层协议软件处理。而且，当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发向与自己不在同一子网(使用了不同的掩码、IP 地址和网关)的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。此外，TCP/IP 协议的设计基于一种非常友好的、通信的双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名和口令等信息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有简单的网络和 TCP/IP 协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。同样，正确使用网络监听技术也可以发现入侵并对入侵者进行追踪定位，在对网络犯罪进行侦查取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。

13.3.2　网络监听实践

确定网络中需要监听的节点后。下载、安装好以下软件，即可实现网络监听。接下来以 Windows 环境为例来介绍。

- WinPcap。建议到其官方网站 http://www.winpcap.org 下载，当前最新稳定版本是 4.1.1。
- Ethereal 或 WireShark。建议到其官方网站 http://www.ethereal.org 以及 http://www.wireshark.org 下载。Ethereal 和 WireShark 的运行需要 WinPcap 的支持，因此需要先安装 WinPcap，再安装 Ethereal 或 WireShark。

安装 Ethereal 后，运行其主程序 Ethereal.exe，出现图 13-2 所示界面。

进行网络监听前，需要先选择网络接口(Interface，网卡)，以决定监听哪块网卡上的数据。操作方法是选择菜单 Capture→Interfaces，如图 13-2 所示。

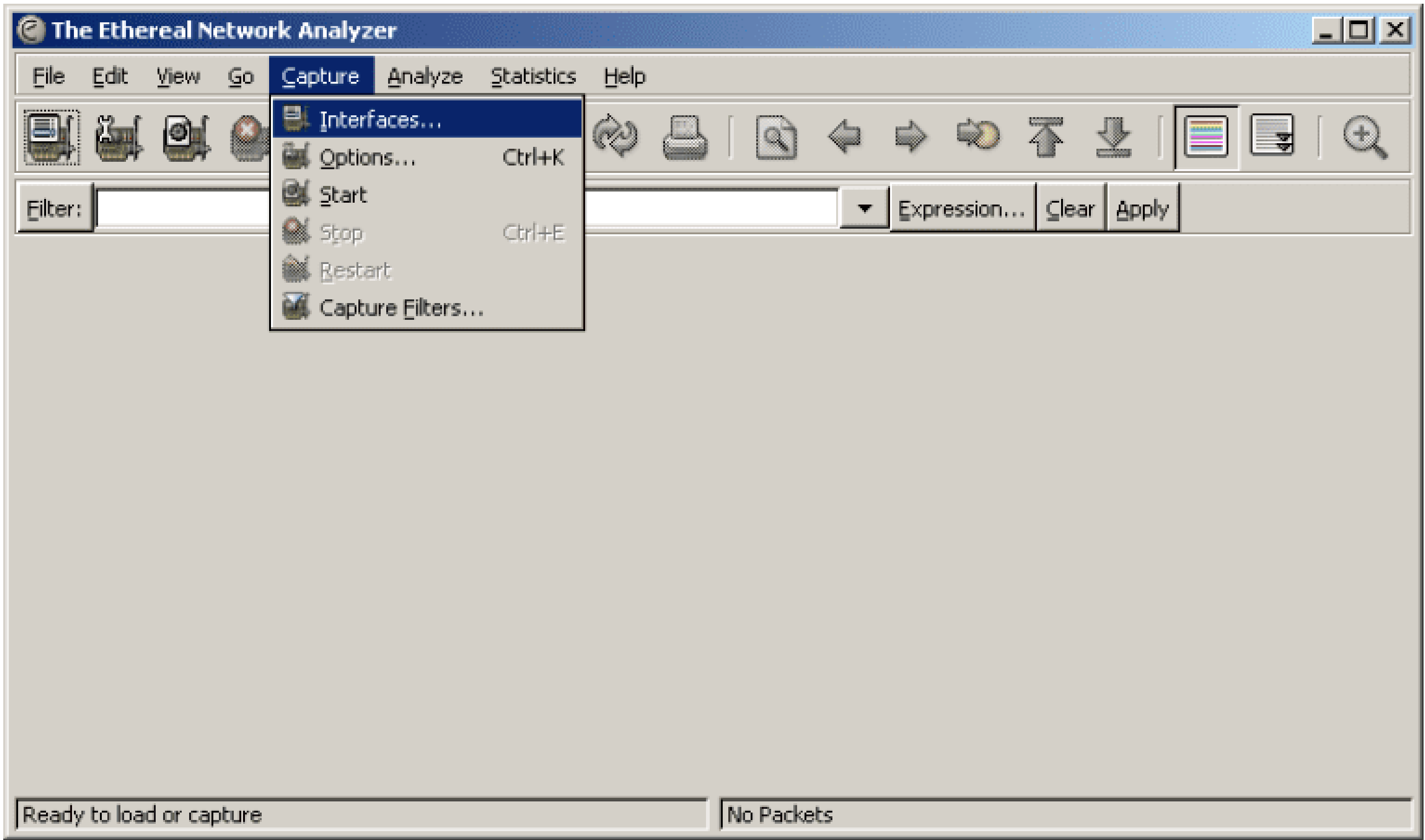


图 13-2　在 Ethereal 中选择准备网卡

当所操作的计算机中有多块网卡时，需要注意正确区分。图 13-3 所示的计算机中，有 Bluetooth PAN、Realtek RTL8187、Reltek RTL8168 三块网卡，其中第二块网卡图标中有个天线符号，表明这是一块无线网卡。用鼠标单击某块网卡时，在状态栏中都会提示该网卡的详细名称。13-3 中选中的是“本地连接”对应的千兆以太网卡——“Realtek RTL8168…Ethernet NIC”。

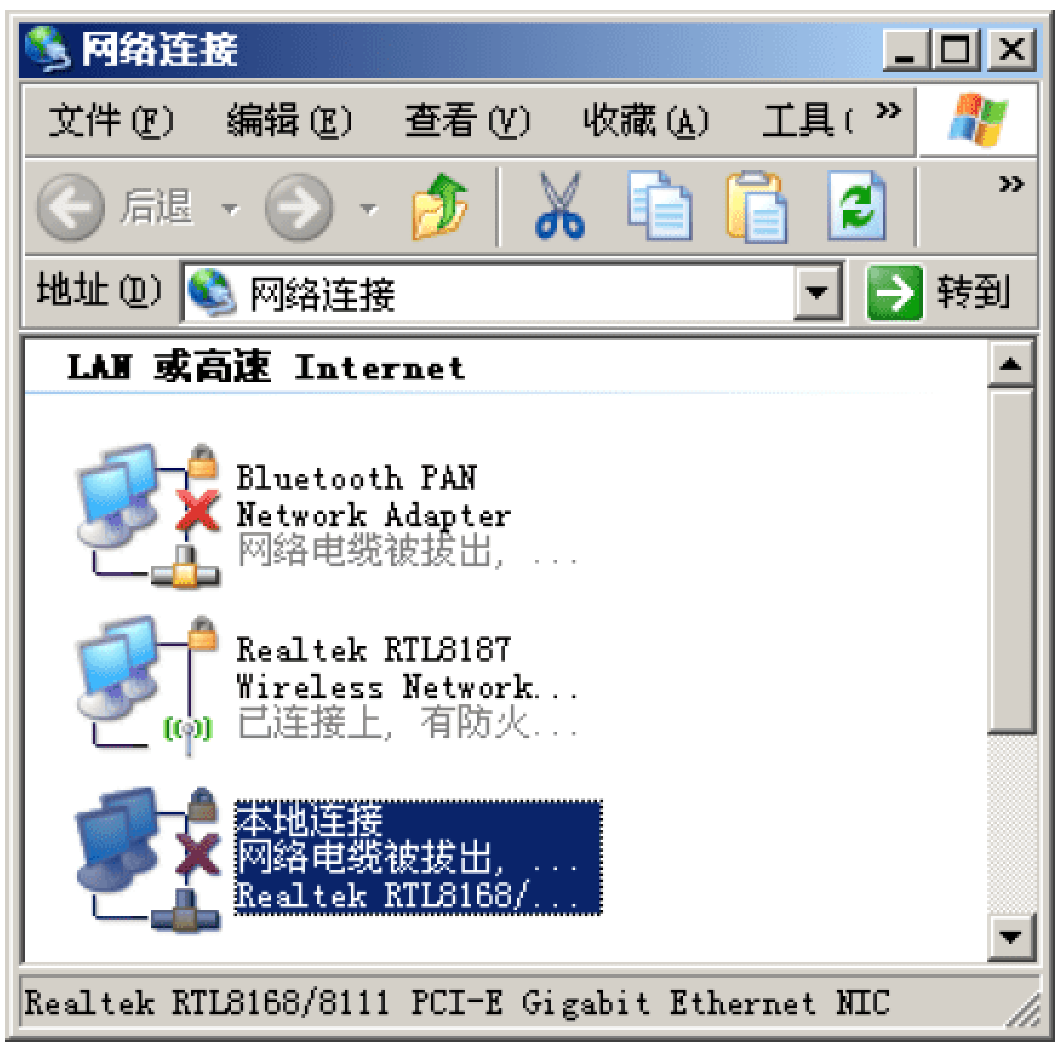


图 13-3　选择正确的网卡

在 Ethereal 弹出的界面中，找到正确的网卡，单击该网卡对应的 Capture 按钮，如图 13-4 所示，即开始监听该网卡上的网络数据。

启动监听后，Ethereal 会出现一个协议统计界面，包含各类协议所捕获到的数据包计数信息以及停止监听的按钮，如图 13-5 所示。

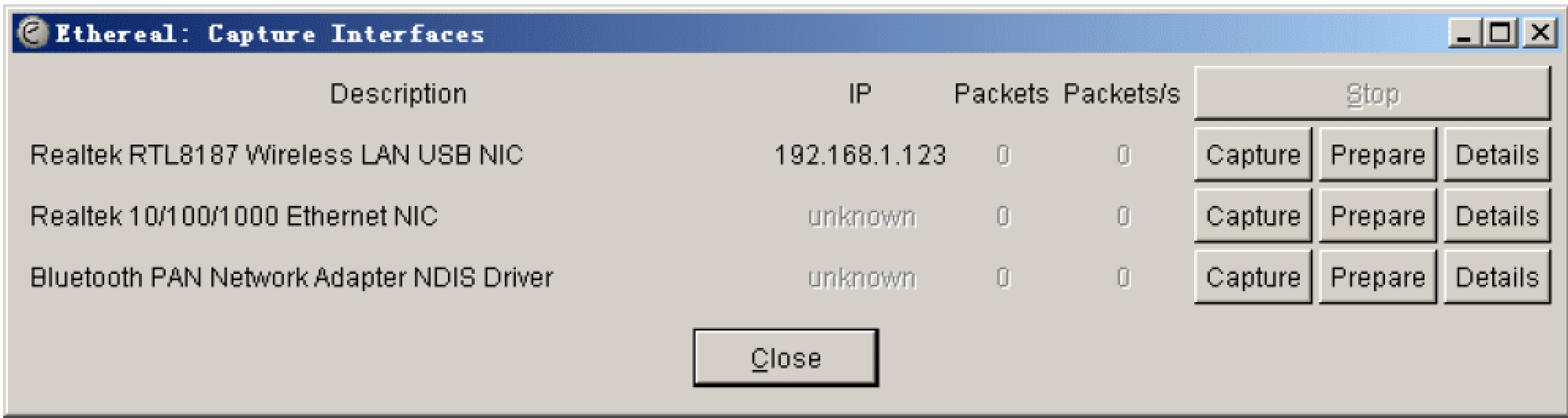


图 13-4　选择正确的网卡监听

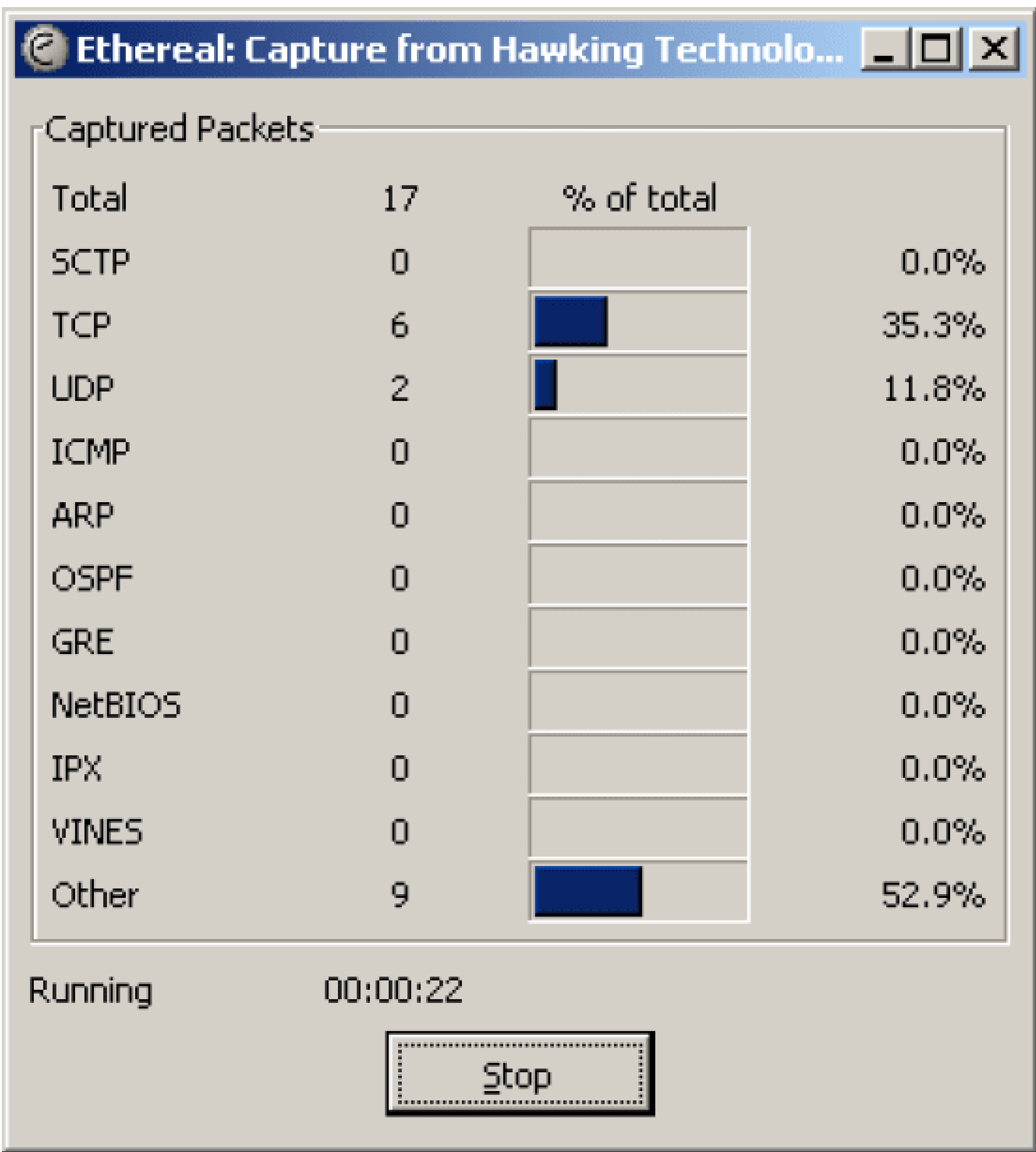


图 13-5　网络监听中的协议数据包统计

需要停止监听时，单击 Stop 按钮，即出现图 13-6 所示的协议数据包分析界面。Ethereal 对网络协议的数据包分析比较细致，图 13-6 界面中分为三个区域，上方包含数据包序号的区域是数据包的序号、时刻信息、源 IP、目的 IP、协议类型、协议概要信息。中部区域是对当前选中的数据包的协议分析，列出了从链路层到网络层、传输层、应用层的协议数据的每一

个字段的分析。图 13-6 的例子是应用层的例子，展示了一次电子邮件登录过程中应用层数据。界面下方区域中是当前数据包的 16 进制数据及这些数据对应的 ASCII 字符。

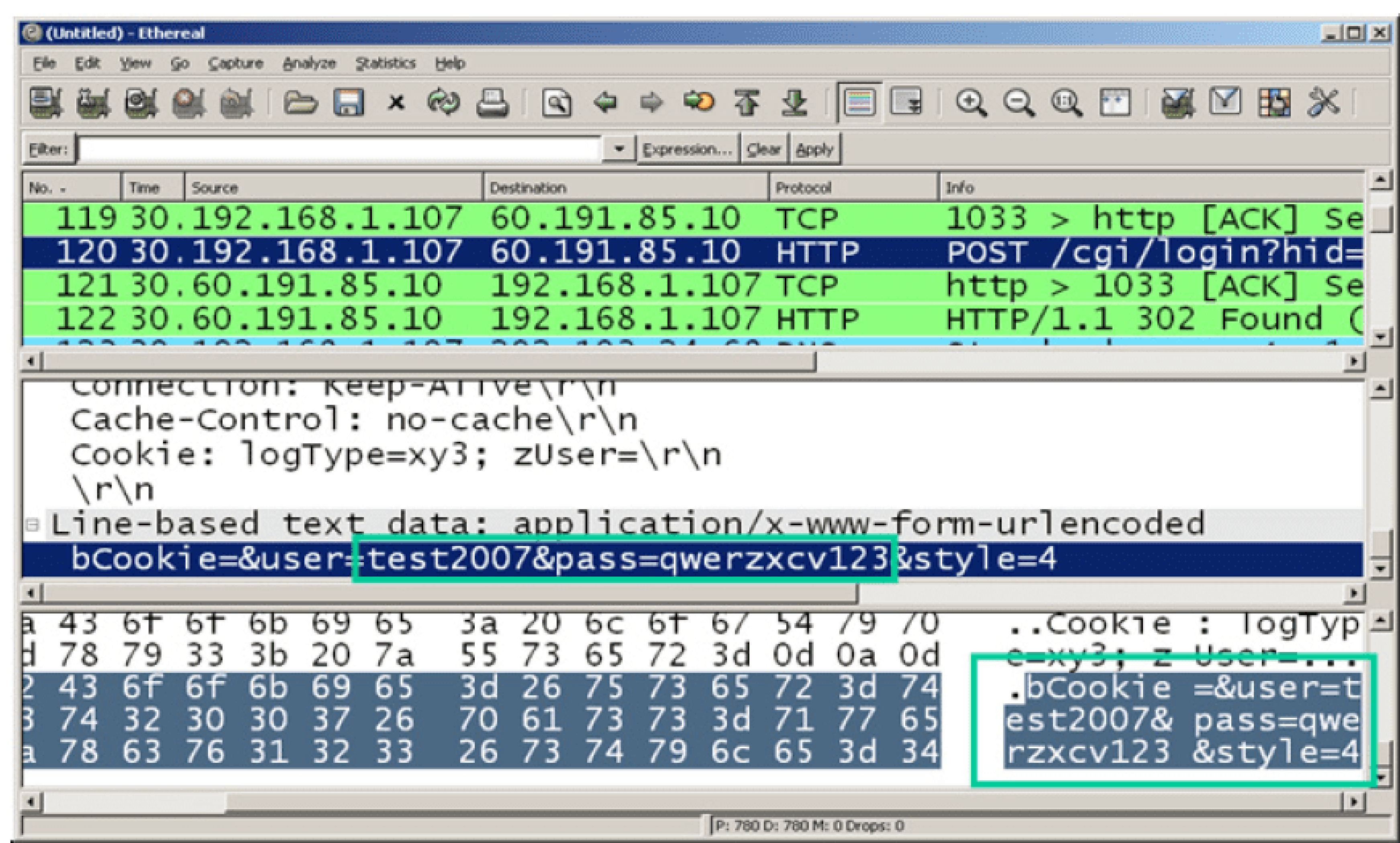


图 13-6　利用网络数据包

13.3.3　网络监听防范

网络监听较难被发现，因为运行网络监听的主机只是被动地接收在局域网上传输的信息，不主动与其他主机交换信息，也没有修改在网上传输的数据包。

可以采取以下措施对可能存在的网络监听进行检测。

- 对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址 ping 该机器，若其运行了监听程序则可能有响应。这是因为正常的机器不接收错误的物理地址，处于监听状态的机器则会接收，且如果该机器的 TCP/IP 协议栈不再次反向检查的话，就会响应。
- 向网上发大量不存在的物理地址的包，由于监听程序要分析和处理大量的数据包会占用很多的 CPU 资源，这将导致性能下降。通过比较前后该机器性能加以判断，这种方法难度比较大。
- 使用反监听工具如 Antisniffer 等进行检测。

要做到对网络监听的比较有效的防范，可采取以下措施。

1. 从逻辑或物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

2. 以交换式集线器(即交换机)代替共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过普通共享式集线器。用共享式集线器连接的网络环境中，两台机器之间传输的数据包(称为单播包，Unicast Packet)还是会被同一台集线器上的其他用户监听。因此，应该用交换机代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法监

听。但是，利用 ARP 欺骗(ARP Spoofing)技术，可以实现交换环境下的网络监听。要防范 ARP 欺骗，需要利用交换机的 MAC 地址绑定功能，但普通非可管理的交换机往往没有这种功能。

3. 使用数据加密技术

数据经过加密后，监听虽然可以得到传送的信息，却无法获取其有效内容。使用加密技术的缺点是影响数据传输速度。

4. 划分 VLAN

运用 VLAN(Virtual LAN，虚拟局域网)技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的攻击。

13.4 网络扫描

网络扫描是一把“双刃剑”。用于善意目的时，网络扫描被称为安全评估，是系统管理员保障系统安全的重要手段。用于恶意目的时，网络扫描则是入侵者入侵前收集信息的基本步骤，目的是为了获取尽可能多的关于目标的各类信息，为后续入侵创造良好条件。

网络扫描工具可以通过执行一些脚本文件来模拟对网络系统进行攻击的行为并记录系统的反应，从而搜索目标网络内的服务器、路由器、交换机和防火墙等设备的类型与版本，以及在这些远程设备上运行的服务，并报告可能存在的脆弱性及漏洞。

13.4.1 网络主机扫描

主机扫描的目的是确定在目标网络上的主机是否可达。这是信息收集的初级阶段，其效果直接影响到后续的扫描。

传统的主机扫描技术利用 ping 命令向目标主机发送 ICMP 数据包，数据包内包含 Echo Request 标记，并等待目标主机回复包含 Echo Reply 标记的 ICMP 数据包。如果能收到回复，则表明目标系统可达(同时说明目标主机存活在网络中)，否则表明目标系统已经不可达或发送的数据包被过滤掉。这种基于 ICMP Echo Request 和 Echo Reply 标记的扫描方式的优点是简单、所有操作系统都支持，但缺点在于这类数据包很容易被防火墙过滤而无法收到 Echo Reply 包。

另一种效率更高的利用 ICMP 协议进行扫描的方式，可以通过并行发送，同时探测多个目标主机，称为 ICMP Sweep 扫描。其实现原理是：将 ICMP 请求包的目标地址设为广播地址或网络地址(注：网络地址也是一个 IP 地址，但这个 IP 代表一个网络地址段，而非代表某台特定的主机或设备)，则可以探测广播域或整个网络范围内的主机。ICMP Sweep 扫描的最大缺点是，只适合于 UNIX/Linux 类操作系统，而 Windows 会忽略这种数据包。此外，这种扫描方式容易引起广播风暴，从而导致网络内的通信阻塞。

防火墙和网络过滤设备常常导致传统的主机扫描技术失效。为了突破这种限制，必须采用一些非常规的手段，利用 ICMP 协议提供网络间传送错误信息的手段，往往可以更有效地

达到扫描目标主机或设备的目的。主要有以下几种方式。

1. 构造异常的 IP 数据包头

向目标主机发送包头错误的 IP 数据包，目标主机或过滤设备会反馈 ICMP Parameter Problem Error(ICMP 参数错误)信息。通常构造错误的 IP 数据包头的字段为 Header Length(头部长度)和 IP Options(IP 选项)。根据 RFC 1122 的规定，主机应该检测 IP 包的 Version Number(版本号)、Checksum(校验和)字段，路由器应该检测 IP 包的 Checksum 字段。不同厂家的路由器和操作系统对这些错误的处理方式不同，返回的结果也各异。结合其他手段，则可初步判断目标系统所在网络过滤设备的过滤规则。

2. 在 IP 头中设置无效的字段值

向目标主机发送的 IP 数据包中填充错误的字段值，目标主机或过滤设备会反馈 ICMP Destination Unreachable(ICMP 目标不可到达)信息。这种方法同样可以探测目标主机和网络设备及其过滤规则。

3. 错误的数据分片

当目标主机接收到错误的数据分片(如某些分片丢失)，且在规定的时间间隔内得不到更正时，将丢弃这些错误数据包，并向发送主机反馈 ICMP Fragment Reassembly Time Exceeded(ICMP 片段重组超时)错误报文。这种方法实现的扫描效果与方法 1、2 类似。

4. 通过超长包探测内部路由器

若构造的数据包长度超过目标系统所在路由器的 MTU(Max Transfer Unit，最大传输单元)且设置禁止分片标志，则该路由器会反馈 Packet needs to be fragmented but DF set(数据包需要分片，但设置了禁止分片标记)差错报文，从而获取目标系统的网络拓扑结构。图 13-7 是用 ping 命令构造长包的一个例子。其中 ping 命令后面的参数“-n 1”表示只发送一个包，参数“-l 1800”表示构造 ICMP 包的数据区长度为 1800 字节。主要注意的是，ICMP 包的头部长 8 个字节，加上 IP 数据包的头部为 20 个字节，因而构造出的这个 IP 数据包总长度为 1800＋8＋20＝1828 字节。而以太网默认的帧数据区 MTU 为 1500 字节，因此构造的这个 IP 数据包无法由一个帧容纳，必须分片。ping 命令的参数“-f”表示在构造的 IP 数据包中设置 DF(Don’t Fragment，禁止分片)。

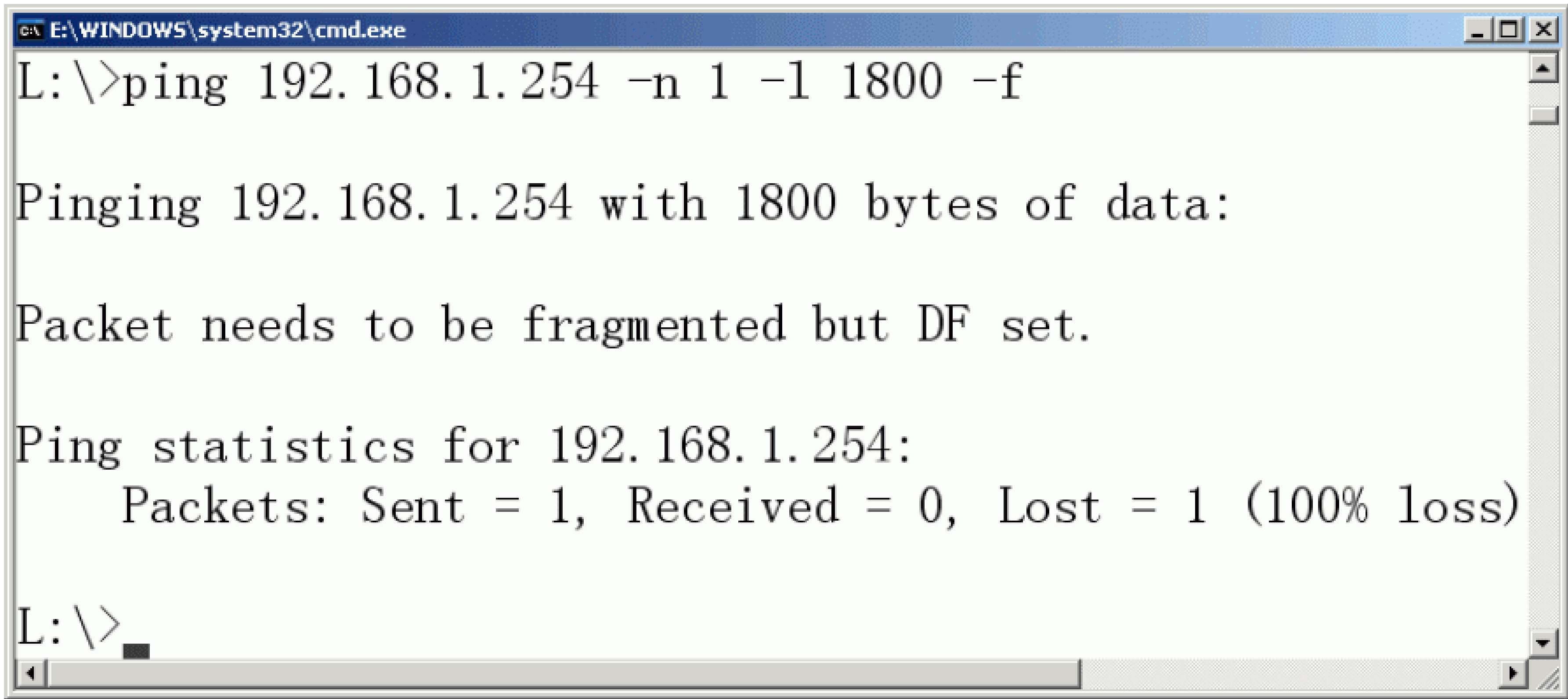


图 13-7　构造长包探测内部路由器

5. 反向映射探测

该技术用于探测被过滤设备或防火墙保护的网络和主机。通常这些目标无法从外部直接到达，但是可以采用反向映射技术，利用目标系统的路由设备进行有效的探测。当我们想探测某个未知网络内部的结构时，可以构造猜测的内部 IP 地址列表，并向这些地址发送数据包。当对方路由器接收到这些数据包时，会进行 IP 识别及路由选择，对不在其服务范围的 IP 包发送 ICMP Host Unreachable(ICMP 主机不可到达)或 ICMP Time Exceeded(ICMP 超时)错误报文，没有接收到相应错误报文的 IP 地址会可被认为存在于该网络中。这种方法的扫描效果会受到过滤设备的影响。

13.4.2　主机端口扫描

当确定了目标主机存活后，就可以使用端口扫描技术，探测目标主机的开放端口，包括网络协议和各种应用监听的端口。端口扫描技术主要包括以下三类。

1. 开放扫描

开放扫描是指扫描过程会尝试建立一个 TCP 连接，若目标端口处于监听状态，则会进行完整的 TCP 三次握手的动作。这种扫描方式稳定可靠，且扫描工具无需具备管理员权限即可运行。但这种扫描方式不隐蔽，服务器日志会记录下大量密集的连接和错误记录，并容易被目标网络的防火墙及安全设备发现和屏蔽。

2. 半开放扫描

半开放扫描分为 TCP SYN 扫描、TCP 间接扫描两种方式。

TCP SYN 扫描的实现原理是，扫描器向目标主机端口发送 TCP SYN 报文。如果应答是 RST 包，说明端口是关闭的；如果应答中包含 SYN 和 ACK 包，说明目标端口处于监听状态，此时再向目标主机发送一个 RST 报文，从而停止建立 TCP 连接。由于在 SYN 扫描时，完整的 TCP 连接尚未建立，所以这种技术通常又被称为半连接扫描。TCP SYN 扫描方式的优点是隐蔽性比开放扫描好，一般系统对这种半扫描很少记录。这种方式的缺点是，通常构造 TCP SYN 数据包需要管理员用户权限。

TCP 间接扫描的实现原理是，利用第三方的 IP(欺骗主机)来隐藏真正扫描者的 IP。由于目标主机会对欺骗主机发送回应信息，所以必须监控欺骗主机的网络通信，从而获得原始扫描的结果。扫描者主机通过伪造第三方主机 IP 地址向目标主机发起 TCP SYN 扫描，并通过观察其 TCP 报文内序列号字段的增长规律，获取目标主机端口的状态。这种方式隐蔽性好，但对第三方主机的要求较高。

3. 隐蔽扫描

隐蔽扫描能有效避免对方入侵检测系统和防火墙的检测，但这种扫描使用的数据包在通过网络时容易被丢弃，从而产生错误的探测信息。隐蔽扫描主要有 TCP FIN 扫描、TCP Xmas 扫描、TCP Null 扫描、分段扫描几种方式。

TCP FIN 扫描的实现原理是，扫描器向目标主机端口发送 TCP FIN 报文，通常此报文到

达一个关闭的端口，报文会被丢掉，并且返回一个 TCP RST 报文。若打开的端口收到 TCP FIN 报文，则直接将其丢弃，而不返回 RST。由于这种技术不包含标准的 TCP 三次握手协议的任何部分，所以无法被记录下来，因而比 TCP SYN 扫描隐蔽得多，TCP FIN 报文能够只监测 TCP SYN 报文的防火墙。但是，跟 TCP SYN 扫描类似，这种方式需要自己构造数据包，要求管理员用户权限。此外，这种方式通常只适用于 UNIX/Linux 类目标主机，但该方法在 Windows 环境下无效，因为不论目标端口是否打开，操作系统都返回 TCP RST 报文。

TCP Xmas 和 TCP Null 扫描是 TCP FIN 扫描的两个变种。TCP Xmas 扫描在发送的 TCP 报文中，设置 FIN、URG 和 PUSH 标记，而 TCP Null 扫描关闭所有标记。这些组合的目的是为了通过对 TCP FIN 标记过滤防火墙等安全设备。当一个报文到达一个关闭的端口，报文会被丢掉，并且返回一个 TCP RST 报文。若是收到打开的端口，则报文只是简单地被丢弃而不返回 RST。基于同样的原因，这种方式有着与 TCP FIN 扫描同样的优点、缺点。

分段扫描并不直接发送 TCP 探测报文，而是将 TCP 报文分成两个较小的 IP 包片段。这样就将一个 TCP 头分成好几个 IP 数据包，从而防火墙等包过滤器就很难探测到。这种扫描方式隐蔽性好，可穿越防火墙。但这种数据包也可能被网络设备丢弃，并且某些程序在处理这些小数据包时会出现异常。

13.5　IP 欺骗攻击

IP 欺骗攻击是在服务器不存在任何漏洞的情况下，通过利用 TCP/IP 协议本身存在的一些缺陷进行攻击的方法，IP 欺骗攻击具有一定的难度，需要掌握有关协议的工作原理和具体的实现方法。

13.5.1　IP 欺骗攻击原理

IP 欺骗利用了主机之间的正常信任关系来发动，所以在介绍 IP 欺骗攻击之前，先说明一下什么是信任关系，信任关系是如何建立的。

在 UNIX 主机中，存在着一种特殊的信任关系。假设有两台主机 HostA 和 HostB，上面各有一个账户 Tomy，在使用中会发现，在 HostA 上操作需要登录 HostA 上的相应账户 Tomy，在 HostB 上操作则必须用 HostB 的账户 Tomy 登录，主机 HostA 和 HostB 把 Tomy 当做两个互不相关的用户，这不够方便。为了简化操作，可以在主机 HostA 和 HostB 中建立起两个账户的相互信任关系。在 HostA 和 HostB 上 Tomy 的 home 目录中创建.rhosts 文件。从主机 HostA 上，在用户 Tomy 的 home 目录中用命令：

```
echo “HostB Tomy” > ~/.hosts
```

即可建立 HostA 与 HostB 间的信任关系，这时，从主机 HostB 上就能毫无阻碍地使用任何以 r 开头的远程调用命令，如 rlogin、rsh、rcp 等，而无需输入口令验证就可以直接登录到 HostA 上。这些命令将允许或者拒绝以 IP 地址为基础的存取服务。这里的信任关系是基于 IP 的地址的。

当/etc/hosts.equiv 中出现一个“+”或者$HOME/.rhosts 中出现“++”时，表明任意地址的主机可以无须口令验证而直接使用 r 命令登录此主机，这是十分危险的，但这是很多管理员容易忽视的地方。下面我们看看 rlogin 的用法。

rlogin 是一个简单的服务程序，它的作用和 telnet 差不多，不同的是 telnet 完全依赖口令验证，而 rlogin 是基于信任关系的验证，其次是进行口令的验证，它使用 TCP 协议进行传输。当用户从一台主机登录到另一台主机上，并且如果目录主机信任它，rlogin 将允许在不需要口令的情况下使用目标主机上的资源，安全验证完便基于源主机的 IP 地址。因此，根据以上所举的例子，我们能利用 rlogin 从 HostB 远程登录到 HostA，而且不会被要求输入口令。

根据以上分析，既然 HostA 和 HostB 之间的信任关系是基于 IP 址建立起来的，那么如能够冒充 HostB 的 IP，就可以使用 rlogin 登录到 HostA，而不需任何口令验证。这就是 IP 欺骗的基本理论依据。但 IP 欺骗的实际实现远没有这么简单。虽然可以通过编程的方法随意改变发出的包的 IP 地址，但 TCP 协议对 IP 进行了进一步的封装，它是一种相对可靠的协议。下面看一次正常的 TCP/IP 会话的过程。

由于 TCP 是面向连接的协议，所以在双方正式传输数据之前，需要用“三次握手”来建立一个可靠的连接。假设还是 HostA 和 HostB 两台主机进行通信，HostB 首先发送带有 SYN 标志的 TCP 报文，通知 HostA 建立 TCP 连接，TCP 的可靠性就是由数据包中的多位控制字来提供的，其中最重要的是数据序号(SYN)和数据确认序号标志(ACK)。B 将 TCP 报头中的 SYN 设为自己本次连接中的初始序号(Initial Sequence Number，ISN)。

当 HostA 收到 HostB 的 SYN 包之后，会发送给 HostB 一个带有 SYN+ACK 标志的 TCP 报文，告之自己的ISN，并确认HostB发送来的第一个数据段，将ACK设置成HostB的SYN+1。

当 HostB 确认收到 HostA 的 SYN+ACK 数据包后，将 ACK 设置成 HostA 的 SYN+1。HostA 收到 HostB 的 ACK 后，完整的 TCP 连接成功建立，双方即可双向传输数据。

根据此过程可知，假如想冒充 HostB 对 HostA 进行攻击，就要先使用 HostB 的 IP 地址发送 SYN 标志给 HostA，但是当 HostA 收到后，并不会把 SYN+ACK 发送到我们的主机上，而是发送到真正的 HostB 上去，这时 IP 欺骗就失败了，因为 HostB 根本没发送 SYN 请求。所以如果要冒充 HostB，首先要让 HostB 失去工作能力，即通过所谓的拒绝服务攻击(Denial of Service，DoS)，设法让 HostB 瘫痪。

但仅仅这样还不够，最难的就是要对 HostA 进行攻击，首先必须知道 HostA 使用的 ISN。TCP 使用的 ISN 是一个 32 位的计数器，从 0 到 4、294、967、295(即 $2^{32}-1$)。TCP 为每一个连接选择一个初始序列号(ISN)，为了防止因为延迟、重传等干扰 TCP 三次握手，ISN 不能随便选取，不同的系统有着不同的算法。理解 TCP 如何分配 ISN 以及 ISN 随时间的变化规律，对于成功进行 IP 欺骗攻击很重要。ISN 约每秒增加 128 000，如果有连接出现，每次连接将把计数器的数值增加 64 000。显然，这使得用于表示 ISN 的 32 位计数器在没有连接的情况下每 9.32 小时复位一次。之所以这样，是因为它有利于最大限度地减少“旧有”的连接信息干扰当前连接。如果 ISN 是随意选择的，那么不能保证现有序例号是不同于先前的。假设有这样一种情况，在一个路由回路中的数据包最终跳出循环，回到“旧有”的连接，显然这会对现有连接产生干扰。预测攻击目标的 ISN 非常困难，且不同操作系统也不相同。

IP 欺骗攻击最困难的地方在于预测 A 的 ISN。攻击难度虽然大，但在某些情况下成功的可能性也很大。例如，入侵者控制了一台由 A 到 B 之间的路由器(假设称为 Z)，则 A 发网到 B 的所有数据，Z 都可以看到，包括 A 发出 TCP 报文中的 ISN，此时攻击显然明显下降。

13.5.2　IP 欺骗攻击防范

对于来自网络外部的 IP 欺骗攻击，防范方法很简单，只需要在局域网的出口路由器上加一个访问控制规则，禁止外部向内部网络的声称来自于网络内部的数据包即可。

对于来自局域网外部的 IP 欺骗攻击的防范则可以使用出口防火墙完成，原理类似出口路由器的设置。但是对于来自内部网络的攻击通过设置防火墙则毫无作用，此时应注意内部网络的路由器是否支持多个接口。如果路由器支持内部网络子网的两个或多个接口，则必须提高警惕，因为它很容易受到 IP 欺骗，这也正是为什么 Web 服务器放在防火墙外面更加安全的原因。

通过对信息包的监控来检查 IP 欺骗攻击是非常有效的方法，使用 netlog 等信息包检查工具对信息的源地址和目的地址进行验证，如果发现信息包来自两个以上的不同地址，则说明系统有可能受到了 IP 欺骗攻击，有来自于防火墙外的入侵企图。

13.6　网络钓鱼攻击

在传统的利用系统漏洞和软件漏洞进行入侵攻击的可能性越来越小的前提下，网络钓鱼已经逐渐成为黑客们趋之若鹜的攻击手段。同时无论网络相关的客户端软件还是大型的 Web 网站都开始发觉网络钓鱼已经成为了一个严峻的问题，并积极防御。

IE 7.0 浏览器开始加入反钓鱼功能，这个功能成为浏览器安全功能的一个选项，仿冒网站筛选器。各类 IM 软件，如 QQ 等开始出现提示用户防止被网络钓鱼的安全信息。电子商务、门户、SNS、BLOG 等大部分 Web 2.0 热门网站也开始公告用户，提醒其防止被网络钓鱼。

13.6.1　网络钓鱼攻击原理

网络钓鱼属于社会工程学攻击的一种，简单的描叙就是通过伪造信息获得受害者的信任并且响应，由于网络信息是呈爆炸性增长的，人们面对各种各样的信息往往难以辨认真伪，依托网络环境进行钓鱼攻击是一种非常可行的攻击手段。

网络钓鱼从攻击角度上分为两种形式，一种是通过伪造具有“概率可信度”的信息来欺骗受害者，这里提到了“概率可信度”这个名词，从逻辑上说，“概率可信度”就是有一定的概率使人信任并且响应，从原理上说，攻击者使用“概率可信度”的信息进行攻击，这类信息在概率内正好吻合了受害者的信任度，受害者就可能直接信任这类信息并且响应。而另外一种则是通过“身份欺骗”信息来进行攻击，攻击者必须掌握一定的信息，利用人与人之间的信任关系，通过伪造身份，使用这类信任关系伪造信息，最终使受害者信任并且响应。

经常出现的是第一种形式的网络钓鱼攻击，比如形形色色的虚假中奖信息等。在今天这个 Web 2.0 大行其道的网络上，使用 Google、百度来查询姓名都有可能得到真实的信息，在

大型的 SNS(Social Networking Service)网络社区，一个名字就能查询出和你所有相关的人的敏感信息，个人隐私几乎已经不复存在。如果这类敏感信息被用作第二种形式的钓鱼攻击，后果将不堪设想。同时这两种形式的攻击原理也被常用作 Web 蠕虫的传播手段，比如利用 Web 应用的消息功能传播蠕虫链接和恶意代码等，当收到朋友的信息时，可能就会直接打开、浏览信息，使蠕虫得以进一步的传播。下面介绍可以被用作网络钓鱼的一些 Web 攻击技术。

1. URL 编码结合钓鱼技术

首先我们要明确一个概念，浏览器除了支持 ASC II 码字符的 URL，还支持 ASC II 码以外的字符，同时支持对所有的字符进行编码。URL 编码就是将字符转换成 16 进制并在前面加上“%”前缀，比如我们将 google 的域名后缀.cn 进行 URL 编码得到：

http://www.google%2E%63%6E

其中，“.cn”这三个字符就是以每个字符的 16 进制形式加上“%”前缀，浏览器和服务端都能够正常支持。攻击者是怎么通过 URL 编码进行钓鱼攻击呢？钓鱼攻击者常用的攻击伎俩就是混淆 URL，通过利用相似的域名和内容来骗取受害者的信任，这里就存在一个相似度的值，通过 URL 编码就能提高 URL 的相似度，假如我们拥有任意一个 y19ml1.cn 这样的域名，使用子域名配合 URL 编码就能提高相似度，比如先制造一个 http://www.google.cn.y19ml1.cn 的子域名，通过 URL 编码将得到如下 URL：

http://www.google.cn%2E%79%31%39%6D%6C%31%2E%63%6E

很容易理解，一个普通用户在浏览信任度极高的网站时，被攻击者使用“概率可信度”信息和“身份欺骗”信息配合相似度极高的 URL，在惯性思维下很难分辨一个 URL 的真伪。

2. Web 漏洞结合钓鱼技术

近两年来，XSS 漏洞开始成为 Web 漏洞中的一个大热门，XSS 漏洞的特性就是能够在网页中插入 JavaScript 代码运行。JavaScript 几乎能做任何事情，传统的 XSS 漏洞攻击可能是直接获取客户端和服务端的会话，可能是制作 Web 蠕虫攻击整个 Web 服务，除利用 XSS 漏洞针对 Web 服务进行直接攻击的风险之外，XSS 漏洞还能被用作钓鱼攻击。为了更深入了解 XSS 钓鱼的危害，这里举一个简单的例子。网页中被插入 JavaScript 运行后，是能够做到直接篡改页面内容的，将如下的 JavaScript 代码放入任何一个已有内容的网页，将清空原有内容，并写入其他内容。

```
window.onload=function Phish(){
document.open();
document.clear();
document.write('Phshing test…');
document.close();
}
```

当钓鱼攻击者利用网站的 Web 漏洞进行钓鱼，网站管理员到这里应该意识到问题的严重性，这类钓鱼攻击并不是针对网站的 Web 服务业务进行攻击，而是利用网站的信任度对网站所有的用户进行攻击。当用户进入自己信任的网站而浏览的却是钓鱼网页，对网站的直接、

间接损害就难以评估了。

3. 伪造 E-mail 地址结合钓鱼技术

伪造 E-mail 地址乍看起来很困难，但是经常接触邮件服务器的技术人员应该知道，我们可以通过邮件代理服务器发送匿名邮件，在没有邮件代理服务器的情况下可以在本地架设服务器发送匿名邮件，甚至可以直接利用 Web 脚本程序使用虚拟主机、Web 服务器的邮件服务发送匿名邮件。通过邮件代理服务器可以直接修改邮件原始信息中 MIME 头的 FROM 字段，也就是发件人地址。利用这种匿名邮件可以伪造任何人的身份发送邮件，如下面的部分原始邮件头信息：

Received:fromlocalhost(unknown[202.103.0.123])

By 192,168.1.1(Postfix)withESMTPid8D20F606002

for;Tue,21June201010:03:08+0800(CST)

Subject: 你中奖了!

MIME-Version:1.0

From: admin@gmail.com

To: test@we.com

MIME 头中的 FROM 字段是可以控制的，这里伪造成了 admin@gmail.com 的地址，而现在很多邮件服务商对这类匿邮件并没有提供防护措施，造成的后果是一个钓鱼攻击者能够伪造任何人、任何官方的身份发送钓鱼邮件，而一个普通用户是完全无法辨认信息真伪的。

4. 浏览器漏洞结合钓鱼技术

浏览器的地址栏欺骗漏洞和跨站脚本漏洞可以实现完美的钓鱼攻击，地址栏欺骗漏洞实现的效果就是攻击者可以在真实的 URL 地址下伪造任意的网页内容，跨站脚本漏洞实现的效果是可以跨域名跨页面修改网站的任意内容，当我们访问一个 URL，返回的却是攻击者可以控制的内容，如果这里伪造是一个钓鱼网页内容，普通用户将无从分辨真伪。

这种钓鱼攻击是最严重的，因为这类攻击利用的是客户端软件漏洞，完全不受服务端程序和网络环境的限制，是网站管理员无法控制的，只能在知道漏洞的情况下积极打上软件补丁，或使用安全软件修补客户端软件的漏洞。

13.6.2　网络钓鱼攻击防范

从防范的角度来看，网络钓鱼攻击主要分为两个方面，一方面是对钓鱼攻击利用的资源进行限制，一般钓鱼攻击所利用的资源是可控的，如 Web 漏洞是 Web 服务提供商可以直接修补的，邮件服务商可以使用域名反向解析邮件发送服务器提醒用户是否收到匿名邮件。利用即时通信软件(QQ、MSN 等)传播的钓鱼 URL 链接是即时通信服务提供商可以封杀的。另一方面是不可控制的行为，比如浏览器漏洞，用户必须及时打上操作系统补丁、应用程序补丁，以防御攻击者直接使用客户端软件漏洞发起的钓鱼攻击，各个安全软件厂商也可以提供修补客户端软件漏洞的功能。同时各大网站应保护所有用户的隐私，及时提醒所有的用户防止钓鱼，提高用户的安全意识，从两个方面积极防御钓鱼攻击。

现在的网络钓鱼攻击并未做到主动防御，但当前国内如 QQ、MSN 等即时通信软件，开始提醒用户不要打开未知的不可信的链接，防止被欺骗。

网络钓鱼攻击还可以通过内容关键字匹配 URL 进行主动检测，当前 Internet 上的网页木马等恶意代码横行，杀毒软件提供了查杀网页恶意代码的功能，这类查杀方式最初是使用恶意代码关键字特征码进行查杀，而网络钓鱼也拥有钓鱼关键字，这些关键字大都具有趋利性质，充满了大量的虚假信息，这类信息也是具有特征的，比如中奖、各类银行账号、虚假电话号码等，可按照杀毒软件的模式建立起一个钓鱼的关键字特征库配合 URL 特征进行匹配分析，在一定程序上主动检测或防御钓鱼攻击。

除使用 Web 攻击技术实施网络钓鱼，攻击者还可以使用网络协议漏洞进行钓鱼，比如网络上泛滥的 ARP 攻击、DNS 劫持、DHCP 劫持漏洞等。总之，网络攻击技术层出不穷，但防御手段也会随着攻击技术不断更新，只有保持积极防御的态度才能做到最大化的防御。当前，我国对于网络钓鱼诈骗的立法还不够完善，一些网络钓鱼诈骗在定罪量刑时仍沿用了传统的定罪量刑标准，不能体现网络犯罪等新型犯罪的特点，比如诈骗金额在 2000 元以下的罪案并没有在《刑法》中量刑，这对于网络钓鱼诈骗金额的小额多量的分布式特性无法很好的取证，还有待相关法律的进一步完善。

13.7 Web 安全

Web 是 Internet 上最为普及、广泛的应用类型。Web 应用具有操作简便、部署及更新便捷的特点，越来越多的应用正在将中心由传统的 C/S(Client/Server，客户端/服务器)结构向 B/S(Browser/Server，浏览器/服务器)结构转移。

Web 应用的迅速普及也带来相关的安全威胁日益严重。近年来，针对 Web 网站的攻击呈现规模化、隐蔽化趋势，并将攻击目标锁定为知名合法网站。2009 年 11 月以来，著名 Web 安全解决方案提供商 WebSense 安全实验室监测到，一场大规模恶意代码注入活动正在蔓延，数万合法网站已经受到攻击，数亿网民受到影响。而对于 Web 安全，用户或多或少存在认识上的误区，无论是对它的危害程度还是企业应该采取的保护方法上都需要有一个清醒的认识。

13.7.1 Web 安全威胁

当前的 Web 应用面临的威胁主要有以下特征。

1. Web 威胁的目标是敏感数据和攫取利益

面对来势汹汹的 Web 威胁，绝大多数企业并没有真正意识到其中的危机。一方面，恶意网站以 600%的年增长速度在迅速增加；另一方面，77%带有恶意代码的 Web 网站是被植入恶意代码的合法网站。如果把前者比作可避免的明枪的话，作为暗箭的后者则可以轻而易举地攻击无辜 Web 用户，进而危及企业网络中的数据。

Web 攻击是目前数据窃取的主要途径。监测结果显示，当前 57%的数据窃取攻击是经由 Web 实现的。由于基于 Web 2.0 的安全威胁具有定向性、隐蔽性和区域性爆发等特点，所以

越来越多的合法网站被挂马(植入木马程序)、被注入(利用 Web 应用程序的漏洞实现对 Web 站点、服务器的入侵及控制)，对此不知情的员工对 Internet 的依赖性使得企业网络比以往更加容易受到攻击，使得一次普通的浏览网页也变成了一件具有很大安全风险的事情。针对 Web 应用的攻击，可以在用户完全没有察觉的情况下进入企业网络，从而对企业数据资产、行业信誉和关键业务构成极大的威胁。即便是一些看上去并不重要的信息片段，一旦被偷窃者汇集并归纳，其后果仍可能导致公司内部机构设置、战略合作伙伴关系、核心客户等重要信息被泄露。

Web 攻击的目标是企业及政府、军事部门的数据，绝大多数的最终目的是为了获取商业利益。Ponemon 研究机构的一项研究也证明了这一点，数据泄露、丢失等破坏行为的平均开销正在逐年增加。并直接给企业带来业务损失，损失占到企业总花费的 69%。Forrester 同样在名为“计算安全信息泄密代价”的调查中发现：三分之一以上的企业都曾遭遇到数据泄漏事件，其中一半公司由于数据泄漏事件付出了惨痛代价。与员工上班玩游戏、炒股、聊天、下载等行为造成工作效率下降、带宽资源紧张相比，Web 攻击造成的损失就是数据泄漏，直接给企业造成经济损失，因而成为当前企业面临的最紧迫的安全问题。

2. 传统防护手段难以防范 Web 应用安全威胁

对付 Web 威胁，传统的防护模式是否能够有效化解呢？答案是否定的。越来越多的 Web 攻击者将合法网站做目标，77%带有恶意代码的 Web 网站是被植入恶意攻击代码的合法网站，甚至某些知名网站也有网页被挂马的案例。即便如此，相关网站的业务必须保持不间断运行，不能因为 Web 站点的安全威胁而利用上网行为管理产品整体封锁整个网站。此外，尽管大多数 Web 2.0 网站自身都会采取防挂马、防注入等保护措施，但是研究结果显示，65%~75%的 YouTube(全球最大的视频短片分享网站)和 BlogSpot(Google 的博客服务)所采用的社区驱动型安全工具在保护 Web 用户避开不良内容以及风险控制方面的效果并不理想。

面对来势汹汹的新型 Web 威胁，传统安全措施无法跟上 Web 内容及应用类型不断变化的步伐。一方面恶意软件也可能出现在声誉良好、受到大家信任的网站上，就像出现在其他网站恶意上一样容易，另一方面网络应用程序越来越多，传统的防护模式已经力不从心，即便是如今已经运用的非常成熟的“病毒特征码查杀”技术，随着病毒爆发的生命周期越来越短，其传统的安全系统防御模型更是滞后于病毒的传播，用户只能处于预防威胁、检测威胁、处理威胁、策略执行的循环之中。即使利用市场上现有最快速的反病毒系统和服务机制，企业仍然不能防范最新的威胁，因为服务方往往无法及早和完整地介入整个新病毒事件。

3. Web 安全和防信息泄露是企业自我保护的基本条件

Web 2.0 改变了企业使用 Internet 的方式。通过诸如 Facebook 和 Twitter 之类的网站，员工可以自己创建内容并迅速与数千人分享。这些网站中的内容是动态的，传统的安全系统无法控制。为了在工作中使用 Web 2.0，企业需要采用新的方式来保护重要信息。

有效的防范 Web 威胁和防止数据泄漏的安全解决方案，应当基于 Web 安全与防信息泄露的有效结合。Web 安全方案可以有效过滤来自 Internet 的风险，将数据窃取的企图消灭在萌芽阶段，而防信息泄露方案可以对企业的信息资源进行针对性的保护。

具体来说，Web 安全方案提供全面的覆盖范围、可见性和控制，对于“谁能够发送什么信息、在哪里发送、如何发送”全部一目了然。数据泄漏防护方案可以识别、监视和保护机密数据。通过将 Web 安全方案与数据泄漏防护方案相结合，企业可以有效控制 Web 风险，精确防止数据泄漏，保护业务流程。

下面是一次典型的利用 SQL 注入漏洞，对一个测试站点的攻击过程。

图 13-8 使用一个内网 IP 地址，架设了一个基于 ASP 程序的测试站点，该站点是一个软件下载站，所使用的 ASP 程序被广泛应用于 Internet 上的其他一些软件下载站点。我们使用 Internet 上的免费 Web 应用安全测试工具对这个站点进行测试。

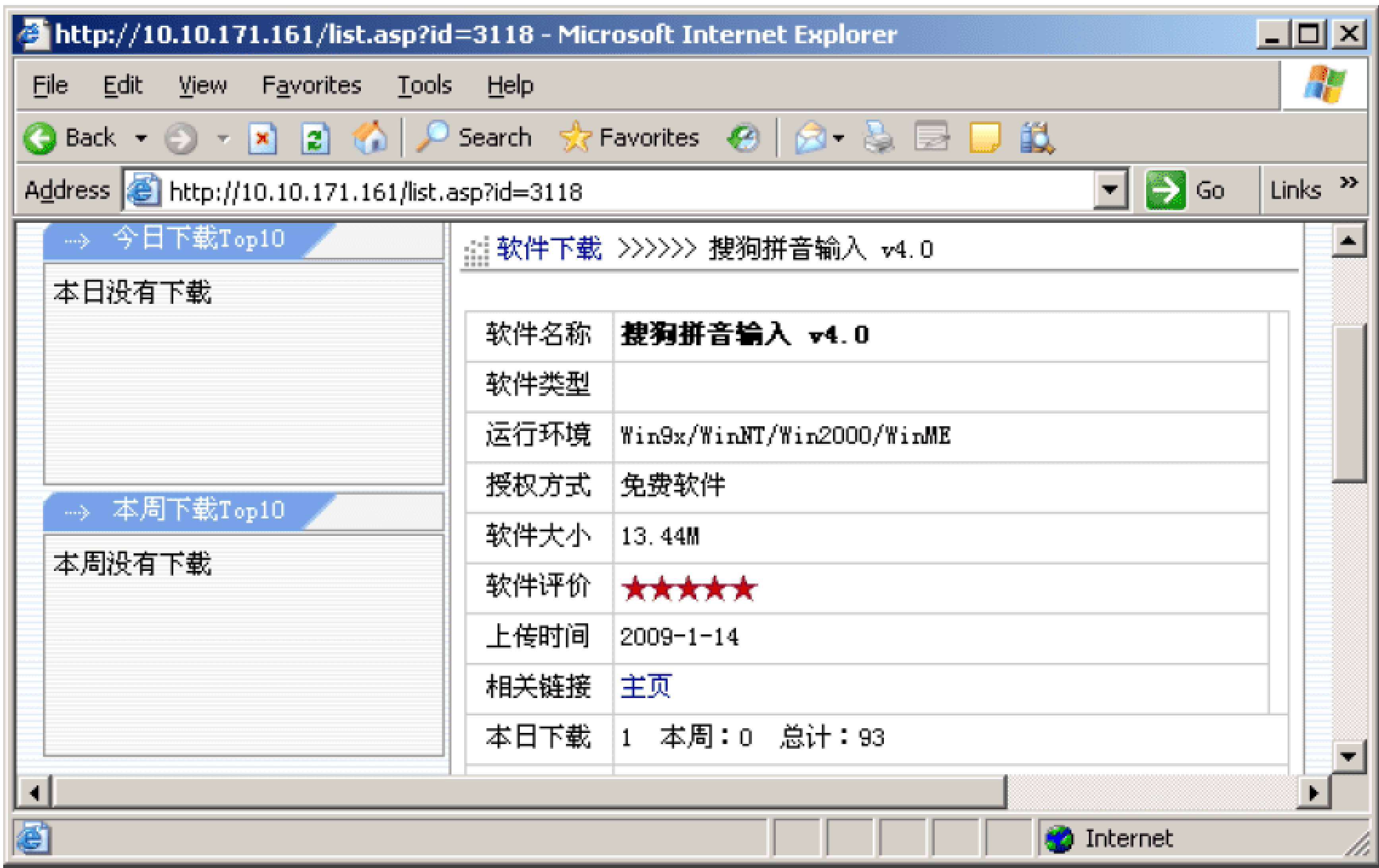


图 13-8　基于 ASP 程序的测试站点

我们使用的 Web 应用测试工具名为 Pangolin，如图 13-9 所示。

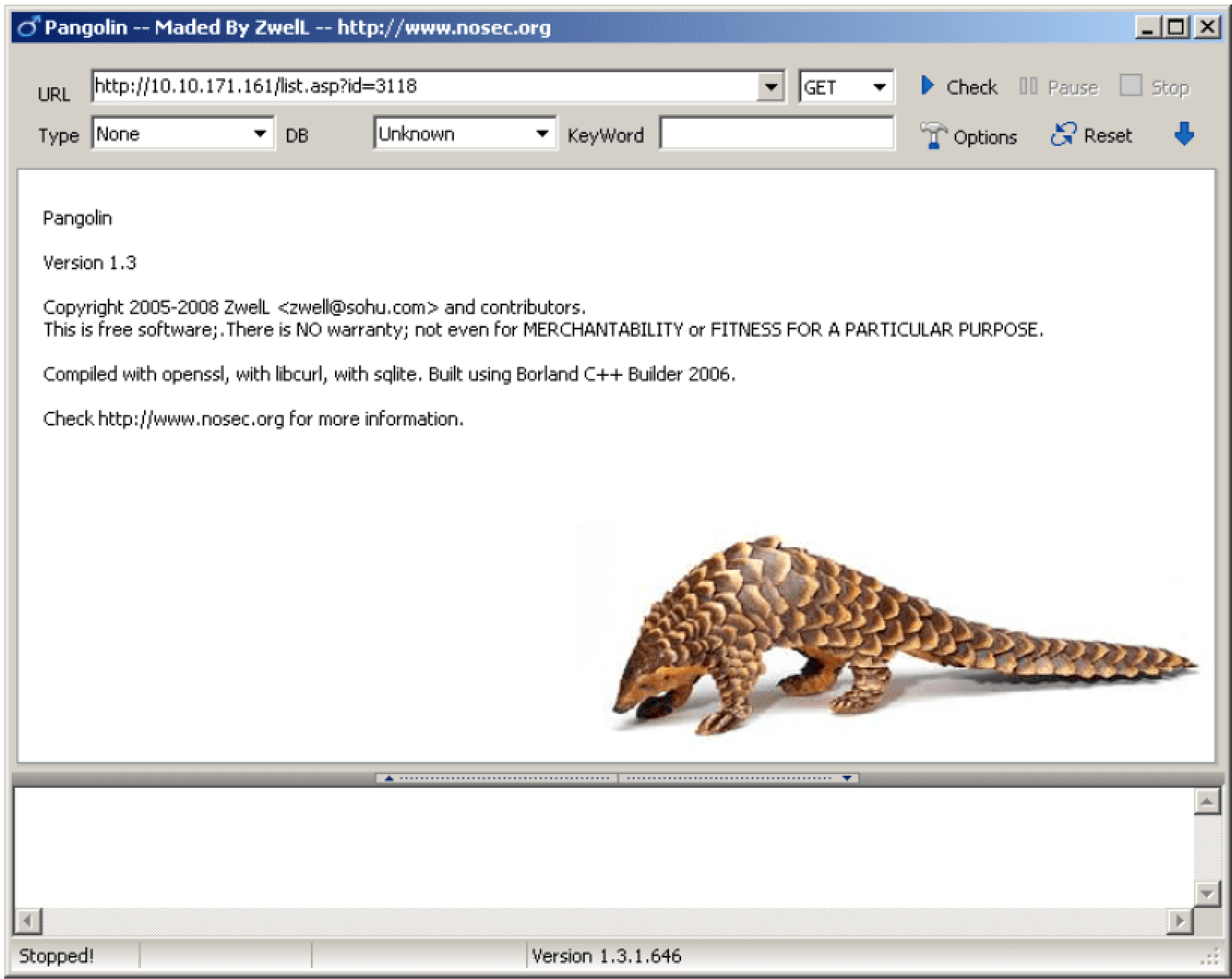


图 13-9　Web 应用测试工具(Pangolin)

Pangolin 的使用非常简单，只需在其界面的 URL 栏中填写目标站点的一个带参数的 URL，然后单击 Check 按钮即可。在本例中，填入图 13-8 界面中显示某软件下载页面的 URL “http://10.10.171.161/list.asp?id=3118”，图 13-9 中已填好此地址。

单击 Check 按钮后数秒，出现图 13-10 所示的界面。

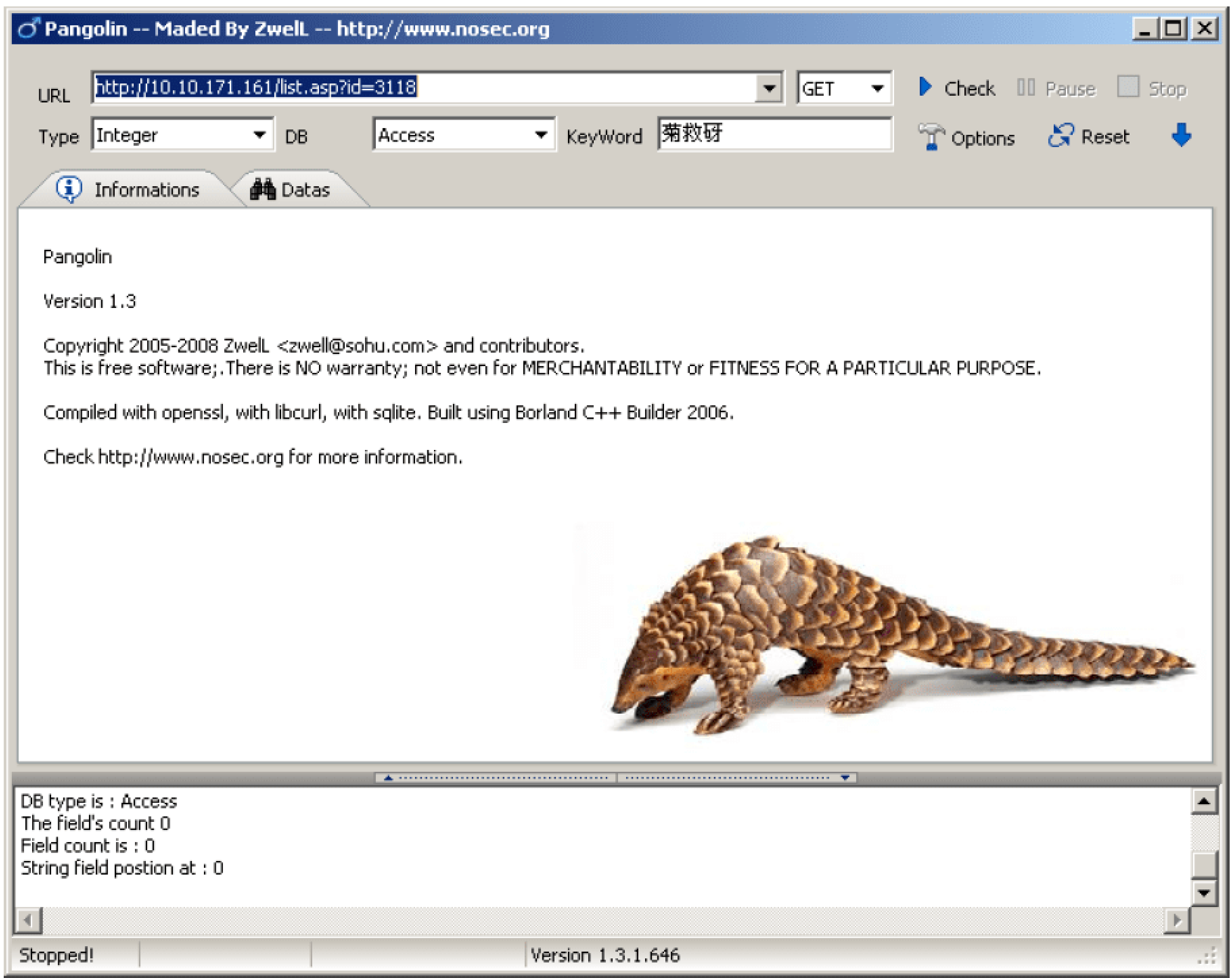


图 13-10　测试目标站点后的主界面(一)

由图 13-10 可见，Pangolin 测试目标站点后，确认站点使用的数据库为 Access，界面中部 Information 栏的右侧出现了一个 Datas 栏，表示可能探测到目标站点的数据库内容。单击“Datas”栏，并在新的界面中单击中下部的 Tables 按钮，则 Pangolin 会尝试获取目标站点数据库内的各个数据表(Table)，成功后就列出在界面中部。

本例中测试结果会得到一个名为 admin 的数据表，双击此表，并选中表中的各个字段 id、username、password，然后单击界面中下部的 Data 按钮，界面见图 13-11。由图 13-11 可见，利用这个免费的 Web 应用测试工具，经过简单的几步操作，就获得了这个网站的管理员用户名、口令。事实上，Internet 上存在类似 Web 应用漏洞的网站相当多，因 Web 应用程序编写不严谨、缺乏基本的安全保护措施导致的网站被攻击的事件在网络安全问题中显得日益突出。

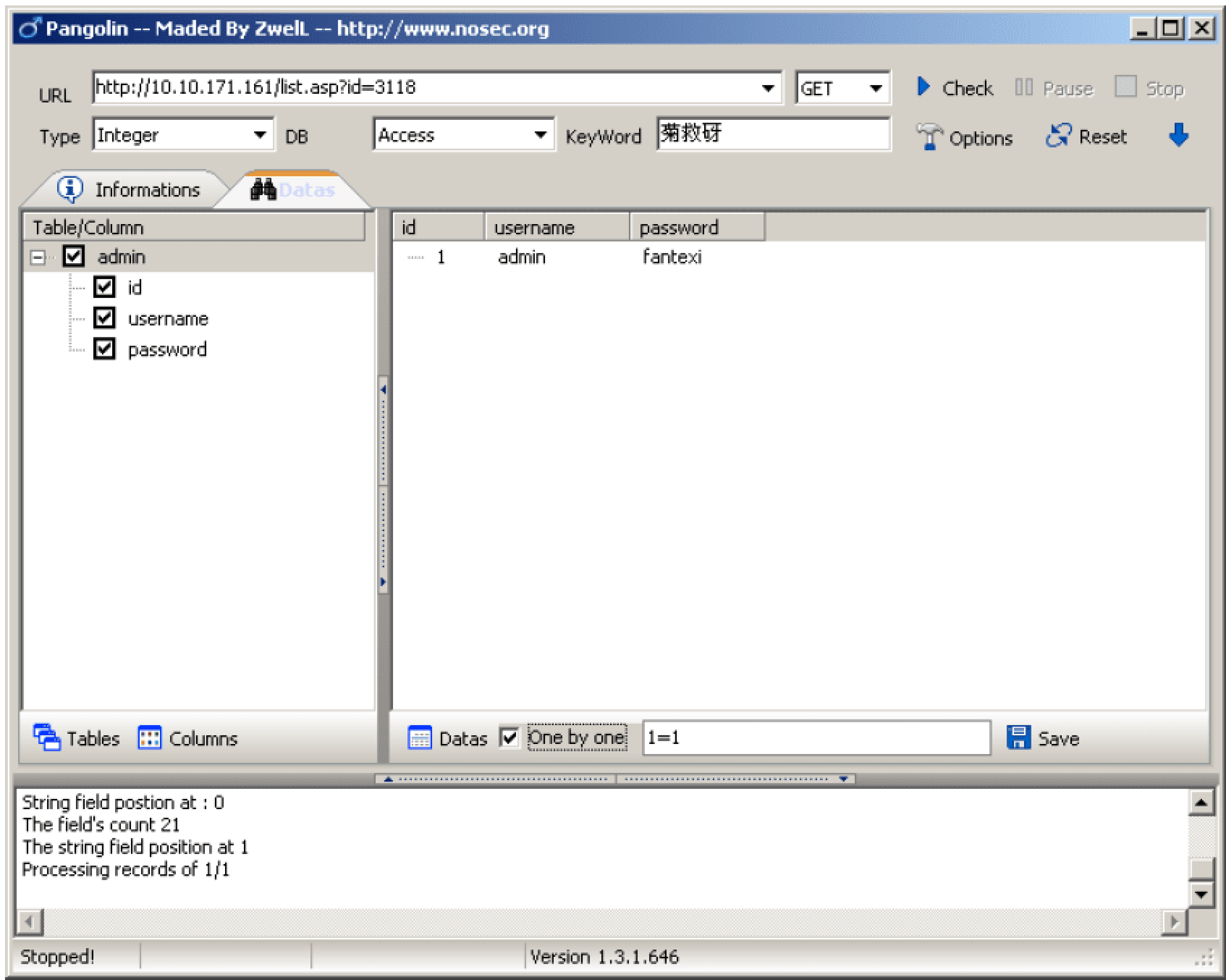


图 13-11　测试目标站点后的主界面(二)

13.7.2　Web 安全防范基础

Web 应用的安全保障需求是无可置疑的，然而，只有先弄明白了自己的站点是如何被攻击的，才可能设法保护它们。Web 应用安全防范的基本要求，就是定期对自己管理的网站进行“渗透测试(Penatration Test)”，渗透测试与攻击者对网站进行攻击的过程非常相似，不同之处主要在于，渗透测试的目的是发现网站的缺陷、漏洞以及时处理和修补，而恶意攻击的目的是为了破坏网站的正常运行或为了经济利益等盗取相关信息及数据。

全面、系统的渗透测试操作，被称为安全评估。针对当前 Web 站点的安全现状，最好的方式就是在部署相应的安全防范安全解决方案的同时，还必须采取与攻击者相同的手段，也就是在网站的运营过程中，不断对它进行安全评估，以此来找到网站中可能存在的脆弱性和漏洞。

对 Web 站点进行安全评估，为了能够达到最终的效果，事先先制定一个切合实际的安全评估方案是十分有意义的。当然，对于一些个人网站，或者只进行一次 Web 站点渗透测试来说，也可以跳过制定安全评估方案这个环节，直接使用系统或 Web 脆弱性检测工具对 Web 站点所在的系统和其本身进行详细的测试。

如果需要对一个 Web 站点进行全面的安全评估，或者需要一个安全评估方案来指导你完成相应的 Web 站点渗透测试任务，那么，我们可以按下列内容来构建一个适合自己实际需求的 Web 站点安全评估方案。首先，为 Web 站点安全评估确定一个最终目标，也就是为什么要这么做，这样做需要达到什么目的。其次，为 Web 站点的安全评估指定安全评估人，并确定安全评估时具体的评估对象，为 Web 站点的安全评估制定具体的时间计划表。如果没有特殊情况，则应当严格按照这张时间表规定的时间对 Web 站点实施安全评估。然后，为 Web 站点的安全评估指定具体的评估工具，并要求评估人员对这些工具进行相应的学习，以达到熟练掌握它们的目的，还必须规定评估人员按时对这些评估软件所依赖的评估漏洞库和软件本身进行不断的更新。接下来，需要确定是将安全评估工具安全装在目标 Web 服务器进行安全评估，还是在专门的硬件设备(例如笔记本电脑)上安装评估软件，然后在使用时再接入目标网络实施评估任务。同时，还需明确具体的安全评估方法，明确安全评估过程中需要注意的操作事项，明确安全评估的规章制度和评估人员责任，规定安全评估结果的记录方式，以及评估报告的上报、存档和检索方式。

Web 站点安全评估方案应当根据实际的网络环境以及站点的具体内容和功能，经过详细的调查和分析，再由安全评估参与人员共同完成。当然，一个实际的 Web 站点安全评估方案，所包括的内容可能比上述所列出的内容要多得多，也详细得多，在这里只是对它们做一个简单的说明，具体内容还需要大家根据实际情况具体补充。

对 Web 站点进行安全评估是 Web 安全防范处理过程中非常重要的一个环节，它应当贯穿站点的整个生命周期。对 Web 站点实施安全评估的目的就是指安全评估人员使用相应的评估工具和技术，经过一系列恰当的方法，对 Web 服务器本身、服务器系统、后台数据库系统及网络中已经实施的安全机制进行全面的检测和评估，以此来检测整个 Web 系统是否还存在漏洞，以及验证实施的安全机制是否有效。并根据最后的评估分析结果，对现有的安全策略进行修订，对实施的安全机制进行补充。

Web 站点安全评估的具体实施涉及四个最关键的因素，它们是安全评估人员、评估工具、评估方法和评估对象。

1. 安全评估人员

安全评估人员应当包括 Web 站点所有者、管理员及安全评估实施人员。安全评估实施人员的技术和经验以及工作态度在一定程度上决定了评估的效果和可信性。

有时，一些 Web 站点不得不将安全评估任务外包给一些具有安全评估资质的第三方机构来完成，这也是一些没有具体的 Web 站点管理员的中小企业 Web 网站经常使用的方式。

还有一些 Web 站点，所有的工作都是由站点管理员一个人来完成，对于这样的 Web 站点安全评估报告，通常只会被他自己接受，也就是用来对站点当前的安全状况进行一次简单的体检，以此做到心中有数。

2. 安全评估工具

安全评估工具需要根据所要评估的具体对象来选择。不同的评估对象，所使用的评估工具是不相同的。这是由于有些安全评估工具只是针对某种服务或软件，有些是针对整个主机或网络的；有些安全评估工具只能在某种操作系统平台下运行，而有些安全评估工具却能在许多流行的操作系统平台下运行。一些安全评估工具是软件方式的，还有一些是以独立的硬件方式存在的；有些安全软件是免费的，而有一些是商业的。由此，要找到一款合适的安全评估工具还真的不是随便选择几样这么简单。并且，其他人认为非常好用的安全评估工具，对于我们自己来说并不见得合适，因此，有时我们需要经过不断的试用才能知道哪几款评估软件才是最适合我们自己的。

幸运的是，现在已经有了许多功能强大的评估工具可供我们选择，这些工具包括以下几个。

1) Nmap

Nmap 是一个网络探测和安全扫描程序，我们可以使用它来扫描 Web 站点所在系统或整个网络，并以此来得到 Web 站点所在系统正在运行及提供的服务，开放的端口，使用的操作系统等信息。Nmap 支持包括 UDP、TCP Connect、TCP SYN、ICMP、TCP FIN 及 TCP ACK 等扫描方式，其中有许多扫描方式还可以用来检测防火墙及 IDS/IPS 等设备的回应情况。

Nmap 能够在类 UNIX 系统及 Windows 系统的终端下以命令方式运行，它的命令执行格式为：nmap [扫描类型] [选项]。

我们可以从 http://nmap.org/网站上下载它的最新版本，以及它的详细说明文档。

2) Nessus

Nessus 同样是一个功能强大的安全检测工具，它允许用户使用插件对它进行功能上的扩展。Nessus 使用一个频繁更新的漏洞库作为安全检测的依据。我们可以到 www.nessus.org 网站上下载到它的免费版本 Nessus 3，以及它的详细使用文档。现在相当数量的安全人员都使用它来对网络或主机系统进行全面安全检测。

3) Nikto

Nikto 是一款开放源代码、功能强大的 Web 脆弱性扫描评估软件，它能对 Web 服务器的多种安全项目进行测试，能在 230 多种服务器上扫描出 2600 多种有潜在危险的文件、CGI

及其他问题。Nikto 使用 LibWhiske 漏洞库，Nikto 目前已成为 Web 站点管理员必备的 Web 安全检测工具之一。

可以到 http://www.cirt.net/网站上下载 Nikto 的最新版本。Nikto 是基于 PERL 开发的程序，所以需要 PERL 环境。因此，当 Nikto 需要在 Windows 系统下使用时，要同时下载并安装 ActiveStatePerl 环境。当需要 Nikto 使用 SSL 的安全方式对 Web 站点进行安全扫描时，还会用到 Net::SSLeayPERL 模式，此时必须保证系统中安装有 OpenSSL。具体安装和使用细节可以参考它们的帮助文档。

另外，还有一个与 Nikto 相似的 Web 脆弱性扫描工具 Wikto，它不仅具有 Nikto 同样的功能，还提供 GUI 图形界面，但只能在 Windows 系统下运行。这个工具可以到 http://www.sensepost.com/research/wikto/下载。

4) N-Stealth

N-Stealth 是 ZMT 公司出品的一款商业的 Web 站点安全扫描软件，同时也有可以免费使用的版本，只是功能没有商业版本的多，漏洞库也不支持自动更新。我们可以到 www.nstalker.com 网站上下载它的最新版本，它可以在 Windows98/ME/2000/XP/2003 系统下运行。

除了上面介绍的安全扫描软件以外，还有一些软件也可以用来进行安全检测工作，包括 X-Scan 3.3、WebInject 1.41 和 AcunetixWVS，以及一款功能全面且性能强大的商业安全扫描软件 ISS Internet Scanner 等。

另外，在使用任何评估工具之前，要先对其漏洞库进行升级更新。这是由于现在大多数安全评估工具都是利用漏洞特征库来进行脆弱性检测的，只有保证它们的漏洞特征库为最新状态，才有可能发现 Web 站点及所依赖的系统可能存在的最新漏洞。

3. 安全评估方法

安全评估方法就是具体的安全评估实施方式，它主要涉及下列五个具体方面。

1) 由外向内测试

这种安全评估方式就是以攻击者的角度从 Web 站点所在网络结构中的外部，对它进行安全扫描工作，以此来检测 Web 站点防范来自互联网远程攻击的能力。此种测试方式可以使用上述评估工具中的 N-Stealth、X-Scan 和 Web Inject 等工具来进行。

2) 由内向外测试

由内向外的安全检测方式是指从 Web 站点所在网络结构的内部，对它进行安全扫描工作。这种安全检测方式主要用来检验 Web 站点对来自内部的攻击防范能力，以及检测对用户权限分配情况和内部数据传输过程中的安全性。此时可使用一些操作系统内部网络命令，例如 Netstat，以及 Hping 和 Nikto、X-Scan、Nmap、AcunetixWVS 等工具来进行完成检测任务。

3) 模拟攻击测试

模拟攻击测试是指在实际的测试过程中并不对 Web 站点所在服务器系统及 Web 应用程序、网络设备进行真正的攻击事件。这种测试方式并不会对 Web 站点的性能产生影响，平时大部分的安全评估工作应当使用模拟攻击的测试方式。

4) 真实攻击测试

当使用模拟攻击测试不能真正检验到网站的安全状况时，就可以使用真实的攻击测试。由于攻击是真实的，会对 Web 站点的性能造成影响，因而这种方式最好在 Web 开发的最初阶段，以及没有 Web 业务的时候进行。现在有很多的网站都会请一些专门的黑客来对自己的站点进行真实的攻击，以便最大程度地检测出 Web 站点中存在的安全漏洞问题。

5) 社会工程攻击测试

有许多人认为社会工程只是攻击者用来进行攻击的一种手段，却不知它也是一种很好的检测企业内部员工及站点管理员反社会工程攻击能力强度的评测工具。我们可以通过电话、手机短信及电子邮件的方式对评测的人员实施与攻击相同的社会工程攻击测试。同样，我们还可以通过直接接触的方式对被评测者进行相应的社会工程攻击测试评估。当我们决定进行社会工程方式的安全评估工作时，最好让可信的第三方来进行，这样才可以达到最好的评估效果。

4. 评估对象

评估对象就是指评估过程中具体的评估实施目标，包括 Web 服务器主机操作系统、Web 应用程序框架、数据库系统及网络基础设施等。

这四个因素是 Web 站点安全评估工作中缺一不可的，缺少任何一个或任何一个出现问题，都会使整个评估工作中断或使评估结果不可信。还有就是评估工具的使用并不一定得一次只使用一种工具，我们可以根据所要评估的对象和评估的内容进行组合应用。毕竟，有时一种工具只在某一个方面比较有效，而且，评估软件还存在误报和漏报的问题，组合使用工具，再加上评估人员根据自己经验的判断，就能将评估结果的有效性提高到最高水平。

当 Web 站点安全评估工作完成后，我们还应当根据安全评估结果，对安全策略进行相应的修订，同时对实施的安全机制进行相应的补充。Web 站点的安全评估工作，在站点没有真正投入运行前，可不断地重复进行检测，直到我们认为已经修补了所有已知的漏洞为止。同时，我们还必须在 Web 站点运营过程当中进行安全评估，以此来发现潜在的安全威胁。

不能忽略的一点是，如今攻击者善于主动分析并发现新的漏洞，这样就对现有的漏洞扫描系统造成了一定的瓶颈，并不能完全解决网站被挂马攻击这种威胁。因此，我们在使用它的同时，还必须使用其他的方式来补充它的不足。

作为 Web 站点的管理者需要通过不断对 Web 站点进行安全评估，以便能先攻击者一步来发现网站中可能存在的脆弱性，以便才能在攻击没有发动前就修补好这些漏洞，这样才有可能最大限度地减少网站被挂马的风险。为了更好地了解安全趋势，我们还可以到 www.cert.org 及 www.securityfocus.comh 订阅最新的安全漏洞的邮件列表，以及时了解每天的安全漏洞信息。

通过经常性地安全评估、渗透测试操作，才能及时掌握 Web 应用面临的威胁，才能及时进行处理。例如，13.7.1 节中介绍的 Web 应用程序漏洞会直接导致网站管理员账号泄漏，进而可能使得攻击者利用管理员权限上传木马、Rootkit 程序等到网站服务器，从而实现对网站服务器的远程隐蔽控制。通过渗透测试了解这个程序漏洞后，有两种补救措施。其一，及

时修改网站程序，查找漏洞所在，例如，严密检查用户向 Web 服务器发出的 URL 请求，过滤 SQL 注入常用的字符，检查 URL 长度是否可疑，然后修补程序漏洞。这种方式在对网站程序进行安全性检查、测试后，程序漏洞补好了，就不用担心被同样的攻击方式入侵。然而，这种方式的缺点在于修改程序周期通常会比较长，而且，修好这个漏洞，很难保证程序其他部分没有别的漏洞，特别是大型的网站，其 Web 应用程序通常由众多程序员共同开发，出现漏洞在所难免。因此，第二种补救措施更值得推荐，这就是利用软件程序或硬件设备，对所有发往 Web 服务器的 URL 请求进行过滤，检查该 URL 的内容构成、特征，从而判断是正常的 Web 请求操作，还是 SQL 注入等攻击操作。因为常见的 Web 应用攻击都有一定的模式和特征，因而这种方式能对被保护网站的所有后台 Web 应用程序起到比较好的保护作用，从而在提高安全性的同时，减少对 Web 应用程序检查的工作量。

安全评估与渗透测试是保障网站安全的重要手段，与此同时传统的防火墙、入侵防御、安全审计系统对网站安全防范也是必不可少的设备。

防火墙能控制对 Web 站点的访问权限，避免非授权访问带来的安全威胁。入侵防御系统则能在网站遭受攻击时及时阻止攻击，减少损失。上述针对 Web 站点 URL 请求进行过滤的设备，就是一类针对特定 Web 应用的入侵防御系统。安全审计系统会详细记录一段时间内网络中的敏感操作，可以在发生特定安全事件后，起到事后分析的作用。

本 章 小 结

本章首先分析了完整入侵过程的基本步骤，阐述了网络应用安全中的两个基本威胁——口令安全和网络数据监听安全。之后对入侵信息搜集过程进行了原理剖析，在此基础上介绍了主机存活扫描、主机端口扫描的目的和意义。通过 IP 欺骗原理的分析，明确了 IP 欺骗攻击的难点和防范要点。通过几个简单的实例，本章重点分析了当前 Internet 面临的主要威胁，即网络钓鱼攻击和 Web 应用安全问题。现实中相当多的用户主机被入侵都是由这两类威胁造成的，值得引起高度注意。

课 后 练 习

一、填空题

1. 查询到目标 IP 地址所经过的各跳路由器的命令是(　　　　　　)。
2. 破解口令时，尝试所有可能字符组合的破解方式称为(　　　　　　)。
3. 传统以太网中，总线上的主机能收到所有其他主机间的通信数据，但通常只保留发给自己的数据。若将网卡设置于(　　　　　　)模式，则会保留收到的所有数据。
4. 开放扫描是指扫描过程会尝试建立一个完整的(　　　　　　)。
5. 利用信任关系实现的 IP 欺骗，主要存在于(　　　　　　)操作系统中。

二、选择题

1. 查询某域名的拥有者、联系方式等信息的命令是(　　)。
   A. Nslookup　　B. Whois　　C. ping 域名　　D. netstat
2. 查询某域名内包含的 MX 记录的命令是(　　)。
   A. Nslookup　　B. Whois　　C. ping 域名　　D. netstat
3. 利用网络数据嗅探，可用轻松获得网络中传输的(　　)口令。
   A. 所有　　B. 电子邮件　　C. 明文　　D. 密文
4. 完成存活主机扫描，最简单的命令是(　　)。
   A. netstat　　B. whois　　C. nslookup　　D. ping
5. 伪装成其他网站，使人上当受骗的攻击称为(　　)。
   A. IP 欺骗攻击　　B. 网络钓鱼攻击
   C. 跨站脚本攻击　　D. 拒绝服务攻击

三、简答题

1. 简述口令破解的几种方法及效果。
2. 网络数据嗅探的基本原理、主要危害是什么？
3. 如何有效防范主机扫描、端口扫描？
4. 防范网络钓鱼攻击的主要方法是什么？
5. 防范 Web 站点 SQL 注入，主要方式有那两种？

第14章　数 据 备 份

备份是为了在系统遇到人为或自然灾难时，能够通过备份的数据对系统进行有效的灾难恢复。没有绝对安全的防护系统，当系统遭受攻击或入侵时，数据被破坏的可能性非常大，对金融、证券以及其他类型企业来说，数据的损失即意味着经济损失，这种损失很多时候是企业不能承受的。企业对信息化系统的依赖，事实上是对系统里流动的数据的依赖，因此数据备份越发显得重要，这正是近年来存储、数据备份行业兴起的原因。

本章重点

- 数据备份分类
- DAS、NAS、SAN 的基本原理、应用场合
- 远程数据备份的分类及特征
- 利用 Ghost 进行数据备份操作

14.1　数据备份概述

14.1.1　数据完整性概念

数据完整性是信息安全的基本要素之一。数据完整性是指在存储、传输信息或数据的过程中，确保信息或数据不被未授权的篡改，或在篡改后能够被迅速发现。

数据完整性的保护，通常使用数字签名或散列(Hash，又称哈希)函数对密文进行运算后，得到一个“数字指纹”，并对数字指纹进行加密运算，在数据到达目的地后，对数据再次“取指纹”运算，核对解密后的指纹，如果指纹一致，表明数据没有任何变动，如果不一致，则表明数据在传输过程中发生了变化。

在信息安全领域，数据完整性的概念常常和保密性相互混淆。以普通 RSA 数据加密算法为例，攻击者或恶意用户在没有获得密钥破解密文的情况下，可以通过对密文进行线性运算，相应改变信息包含数据的值。例如交易金额为 X 元，通过对密文乘 2，就可以使交易金额成为 2X。

与保护数据保密性使用各种加密算法不同，保护数据完整性的算法并非加密算法，而是一种“校验”算法。这意味着数字签名、哈希函数对数据的运算并非是双向可逆的过程。使用加密算法对明文数据进行加密运算后，只要掌握了相关密钥，数据即可用对应的解密算法

进行解密，从而还原成明文。而数字签名算法、各种哈希函数算法，对明文数据进行运算后，通常得到同样长度的一段数据，可以理解为原始明文数据的“指纹”，不同的明文数据对应不同的指纹，但是无法利用指纹还原成原始的明文数据。并且，当算法一定时，指纹的长度确定，与原始明文数据的长度无关。也就是说，1 个字节的数据，与 1TB 的数据，在确定的算法下，其指纹长度是一致的。

数据完整性与数据保密性不仅概念容易被混淆，而且数据完整性的重要地位也容易被忽视。典型的错误观点是，数据保密性重要，数据完整性不那么重要。事实上，在很多场合，没有数据完整性的保障，安全就无从谈起。例如，要从某操作系统或应用程序的官方网站下载补丁文件，必须保证下载到的补丁文件是“官方”版本的，即该补丁未经过任何未授权的改动，这样的补丁才能放心使用。因为攻击者完全可以使用中间人攻击(原理见 1.3.2 节)的方式，修改并替换用户下载到的补丁文件，此时用户下载到的文件是被捆绑了木马或 Rootkit 的补丁，用户在运行补丁文件的同时，捆绑的恶意软件同时就被执行并入侵了用户计算机。因此，在专业的软件下载站点中，在提供可下载的文件的同时，还要提供该文件的“指纹”，通常使用的哈希算法有 MD5(Message Digest 5，报文摘要算法 5)、SHA-1(Secure Hash Algorithm 1，安全哈希算法 1)等，如图 14-1 所示。



文件信息

此修补程序的英文版具有的文件属性 （或更新的文件属性） 在下表中列出。日期和时间对这些文件列出在协调世界时 (UTC)。当您查看文件信息时，将转换为本地时间。若要 UTC 与本地时间之间的时差使用控制面板中的 **日期和时间** 项中的 **时区** 选项卡。

动态 Microsoft CRM 服务器

展开该表格

文件的名称	文件版本	文件大小	日期	时间	哈希值
Sdtransform.dll	3.0.5300.1639	128,360	2007年七月21日	02:01	MD5： 34EB8B18B272BF591B5B09F1804A6 SHA1： 9AB263A7B909BF59E3DBB533071790CECEE

图 14-1　软件下载站点提供文件的校验值

用户从网上下载文件后，再对该文件进行哈希运算，把得到的 MD5 或 SHA-1 校验值与官方网站提供的进行比较，即可确认该文件是否是未经任何修改的原始文件。

此外，数据完整性的应用，还充分体现在用户数据备份、恢复应用中。在大多数情况下，备份的数据需要恢复成和原始数据完全相同的状态。而确认数据恢复后是否和备份时的每一个字节、每一个二进制位都相同的工作，正是由数据完整性的相关机制和算法来保障的。因此，数据完整性提供了有效检查、甄别数据备份过程中出现的各种人为及非人为数据差错的手段。

14.1.2　保护数据完整性的方法

目前，数据文件的完整性可以通过哈希值计算、数字签名跟踪和文件修改跟踪这几种方式来保障。通过哈希值计算实现文件完整性的例子如图 14-2 所示。

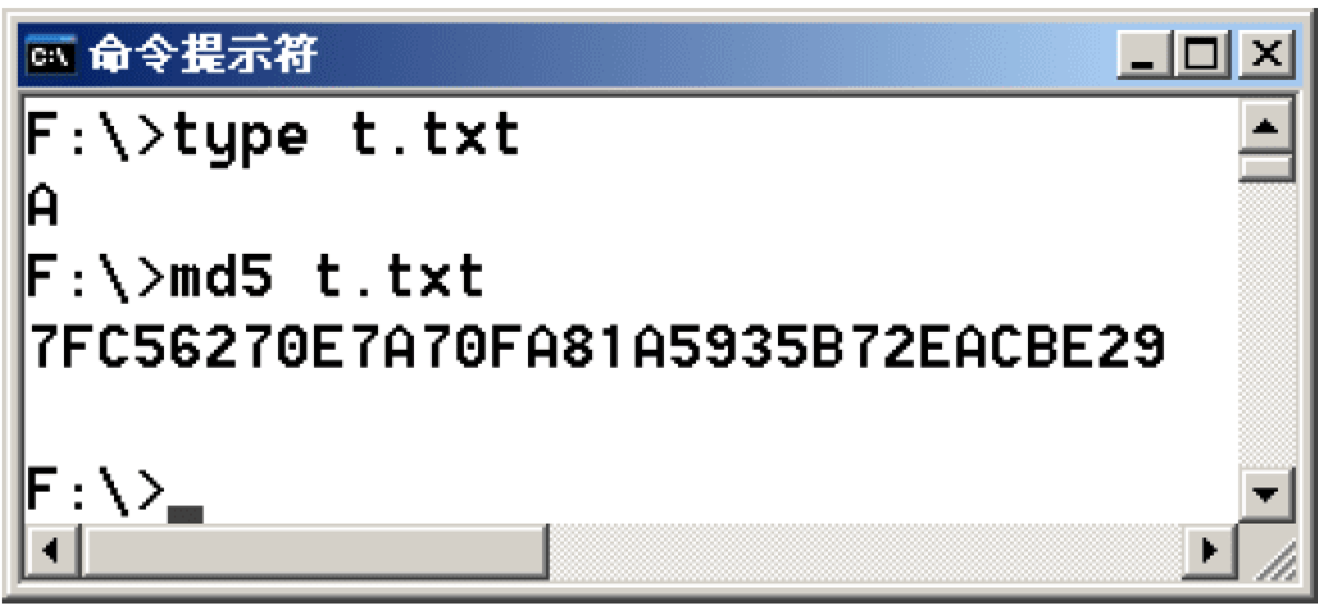


图 14-2　MD5 运算

由图 14-2 可见，文件“t.txt”内容仅为一个英文字符“A”，利用 MD5 运算工具对其进行哈希运算，其结果为一个 16 字节(128 比特)的数字。我们用类似的方法对该文件进行 SHA-1 哈希运算，结果如图 14-3 所示，可知 SHA-1 运算结果为 20 字节(160 比特)。

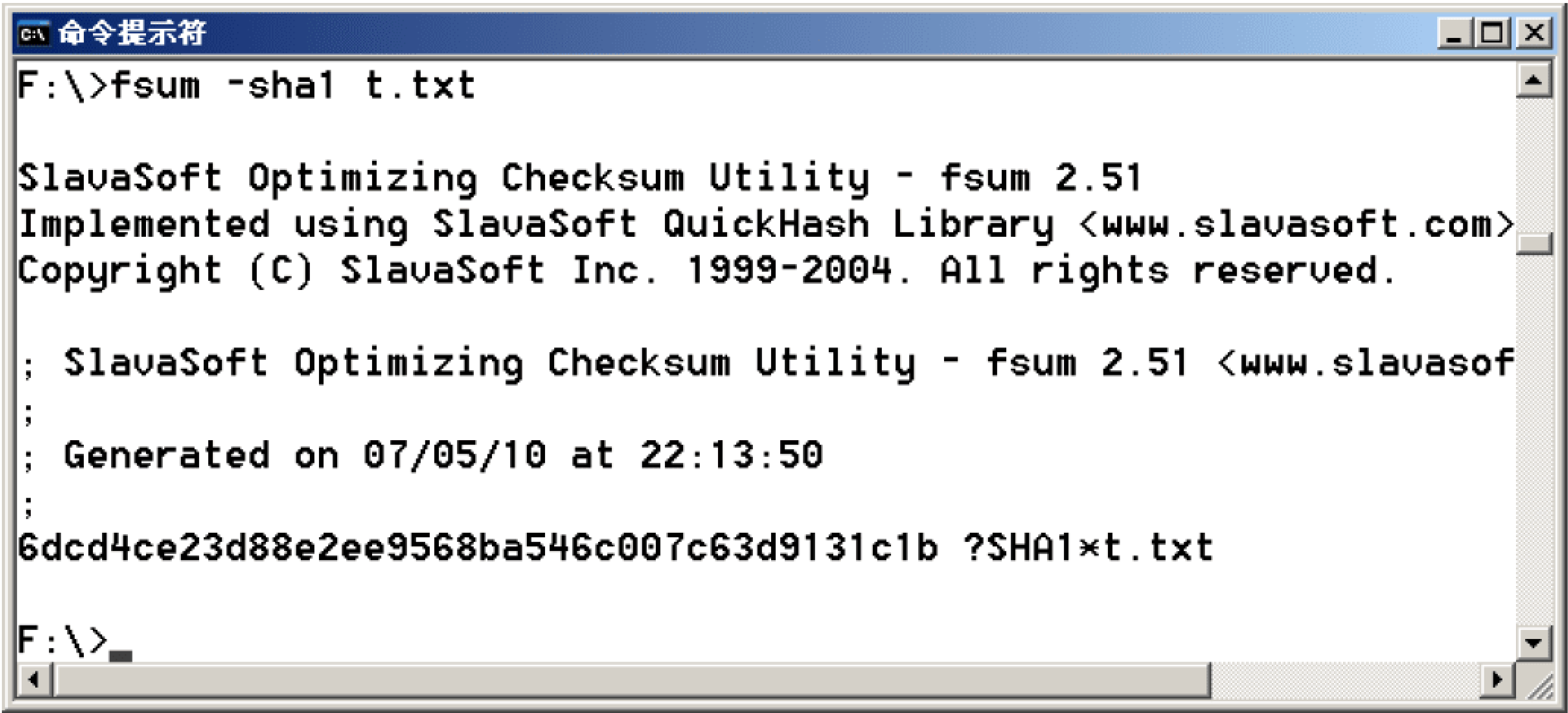


图 14-3　SHA-1 运算

使用数字签名对数据完整性进行保护的机制不同，数字签名采用的是非对称密钥体制，通常用数据发送方的私钥进行签名，接收方收到数据后，用发送方的公钥核对签名，若用发送方的公钥可以对数据进行解密，则意味着签名有效。数字签名实现数据完整性保护的详细原理参见 10.2 节。

MD5、SHA-1 都是基于较复杂的算法，需要使用比较密集的资源才能保证一台计算机上所有文件的完整性，而执行和文件修改跟踪方法则显得有些不可靠，因为现在的许多恶意软件都能够通过修改时间来隐藏对文件的修改痕迹。

由此可见，“标准的”完整性控制方法要么会消耗太多的系统资源，要么会漏掉受感染的文件，这很容易导致恶意软件的扩散传播。而国际上最新的数据完整性保护技术能够避免目前标准中所存在的上述缺点。新技术能够可靠、迅速地查看文件的完整性，并且不会造成过多的资源消耗。

这种新的数据完整性保护技术建立在对应用程序请求进行中途拦截的基础上，这些请求会对一个或多个文件的时间戳进行修改。这类请求可以被每一个文件追踪到并被存储在数据库中。该信息被收集后便会被提供给一个特殊的模块(通常是安全程序中的一个模块)，这个模块会比较时间戳更新及相应时间戳之间发生的变化。从这样的变化可以看出文件是否被修改以及可能的感染。安全程序就可以扫描文件的恶意代码或显示警报。

凭借新一代的数据完整性保护技术，新型的安全产品能够快速、可靠地追查出文件是否

被修改，而该技术还可以对反病毒扫描进行控制，以防止恶意代码的执行。美国 *Network World* 安全专栏作家曾撰文指出，这种技术最大的优势是迅速，仅消耗最少的系统资源就可以完成文件扫描。这项技术使安全网关、反病毒软件等产品的运行更加透明，从而提供更高水平的安全保护。

14.1.3　数据备份系统的组成

在信息技术与数据管理领域，备份指将文件系统或数据库系统中的数据加以复制，一旦发生灾难或错误操作时，得以方便而及时地恢复系统的有效数据和正常运作。

数据备份系统由备份硬件和备份软件两个部分组成。和普通计算机系统的硬件和软件的关系类似，两者是密不可分的，备份硬件是备份软件运行的平台，备份软件是流动于备份硬件中的程序和数据。

1. 备份硬件

备份硬件指的是存储备份信息的设备，它包括硬盘介质存储、光盘介质存储和磁带存储。常见的磁盘方式有磁盘阵列和磁盘冗余。磁盘阵列是 RAID(Redundant Array of Independent Disks，独立磁盘冗余阵列)的中文名称，也就是将多个物理磁盘组成一个逻辑磁盘。RAID 用于提高数据性能、可靠性和可用性，并且 RAID 执行的功能对于操作系统是透明的，不同等级的 RAID 提供不同的速度和不同程度的数据保护。目前 RAID 级别常用的有 RAID 0、RAID 1、RAID 5、RAID 10 等。虽然 RAID 也可用软件实现，但实际生产环境中，为了提高运行效率，通常使用硬件 RAID 卡(又称陈列卡)来实现。

RAID 0 使用一种名为“条带”(Striping)的技术把数据分布到各个磁盘上，每个条带被分散到磁盘的连续数据块上。条带允许从多个磁盘上同时存取信息，可以平衡磁盘间的 I/O 负载，从而达到最快的存取速度。RAID 0 是唯一没有数据冗余的 RAID 级别，这个特性使 RAID 0 除了速度外还有低成本(不会因为冗余空间造成成本上升)的优点，但这也意味着如果阵列中某个磁盘失败，该阵列上的所有数据都将丢失。

RAID 1 是将两个硬盘划分为两部分，一个存数据，另一个做备份。使用这种方法，数据安全性最好，但是磁盘的可用空间只有物理盘空间的一半，利用率比较低。RAID 1 也被称为镜像 RAID，因为一个磁盘上的数据被完全复制到另一个磁盘上。如果一个磁盘失效，另一个还可用。

RAID 5 也被叫做带分布式奇偶位的条带，每个条带片上都有相当于一个“块”那么大的地方被用来存放奇偶位。RAID 5 像分布条带片上的数据那样把奇偶位信息也分布在所有的磁盘上。尽管有一些容量上的损失，但 RAID 5 能提供最佳的整体性能，因而也是最广泛的一种数据保护方案。它适合于 I/O 密集、高读/写率的应用程序，如事务处理等。为了具有 RAID 5 级的冗余度，需要最少由三个磁盘组成的磁盘阵列(不包括热备盘)。在 RAID 5 磁盘组中，任意一块盘出现故障，都不会造成数据丢失。同时出现两块或两块以上的磁盘故障才会损坏数据。RAID 5 是一种综合性能、数据可靠性、性价比的磁盘冗余方式，因而是实际应用中使用最多的一种。

RAID 10 也被称为镜像阵列条带。像 RAID 0 一样，数据跨磁盘抽取，像 RAID 1 一样，

每个磁盘都有一个镜像磁盘。RAID 10 提供 100%的数据冗余，支持更大的卷尺寸，但价格也相对较高。对大多数只要求具有冗余度而不必考虑价格的应用来说，RAID 10 提供了最好的性能。而且使用 RAID 10，可以获得更好的可靠性，因为即使两个物理驱动器发生故障(每个阵列中一个)，数据仍然可以得到保护。RAID 10 需要至少 4 个磁盘驱动器，而且只能通过硬件阵列卡实现。

2. 备份软件

数据备份软件技术就是以软件的方式来实现，将跨平台存储的分散数据提取出来(包括静态和动态的数据)，通过网络(IP Network 或 FC SAN)集中备份到一个或数个大容量存储设备中(如磁盘阵列、磁带库或光盘库等)。一旦源数据受损，就可以从原先备份的介质中恢复。数据备份软件的技术要点包括数据的提取和重导入、数据网络传输、数据转存、集中控制与自动化处理等。

备份软件脱胎于数据存储软件，最初只是简单地将源数据从一个介质转存到另一个介质中。但随着信息技术的不断发展以及在各行各业的深入应用，许多问题也应运而生。数据从原先的单机存储演变为目前的网络多机、多平台分散存储，这就需要建立集中化的网络备份架构；备份的数据从以前的以 MB 计到以 GB 计直至现在拥有上 TB 数据的环境也不罕见，这就对数据的传输和存储提出了高要求；大多数需要备份的信息以动态应用数据的形式组织存储，而非简单的静态数据，这些数据之间还存在关联，于是数据的提取工作就变得相当复杂。

数据备份技术就是针对这些现实应用环境的需求，实现分散数据的网络集中备份，各类应用产生的动态数据的在线提取，多种网络环境下的数据传输，以及跨平台主机、各类存储设备和备份数据自动化管理等。

数据备份软件是进行系统信息备份的主要部分，一款好的备份软件决定了数据备份的效率、安全性等很多方面。目前的备份软件分为专业和非专业两大类。非专业的备份软件主要分布在操作系统厂商提供的软件包中，如 Netware 操作系统的 Backup 功能、Windows 操作系统的 NTBackup 等。专业的备份软件主要集中在数据库类的大型软件中。另外，一些软件厂商提供了全面的专业备份软件，如 Symantec 公司的 NetBackup、HP 公司的 OpenView OmniBack II 和 CA 公司的 ARCServeIT 等。

专业的备份软件能实现异构环境的数据保护，可在异构操作系统、应用程序、管理程序以及磁盘和磁带架构上实现数据保护，并通过内置的复制功能和异地磁带管理功能实现全自动的集成式系统恢复。

14.1.4　数据备份分类

数据备份技术不仅是数据的保护，其最终目的是为了在系统遇到人为或自然灾难时，能够通过备份内容对系统进行有效的灾难恢复。备份不是单纯的复制，管理也是备份的重要组成部分。管理包括备份的可计划性、磁带机的自动化操作、历史记录的保存以及日志记录等。

数据备份技术有多种实现形式，从不同的角度可以对备份进行不同的分类。

1. 按备份模式，可分为物理备份和逻辑备份

逻辑备份指每个文件都是由不同的逻辑块组成的，每一个逻辑的文件块存储在连续的物理磁盘块上。但是，组成一个文件的不同逻辑块极有可能存储在分散的磁盘块上。比如 UNIX 系统，它使用了索引节点(inode)结构来映射逻辑块地址和磁盘上对应的物理地址。一个 inode 包含了指向物理磁盘块的指针。对于比较大的文件，一个单一的 inode 太小，无法映射所有的逻辑块，需要多个块的间接引用包含更多的指针。备份软件通常既可以进行文件操作，又可以对磁盘块进行操作。基于文件的备份能识别文件结构，并复制所有文件和目录到备份媒介上。这样的系统跨越了存储在每个 inode 上的指针，顺序地读取每个文件的物理块。然后备份软件连续将文件写入到备份媒介上。这样的备份使得每个单独文件的恢复变得很快。但是，连续的存储文件会使得备份速度减慢，因为在对非连续存储在磁盘上的文件进行备份时需要额外的查找操作。这些额外的查找操作增加了磁盘的开销。基于文件的逻辑备份的另一个缺点就是对于文件的一个很小的改变也需要备份整个文件。

物理备份与逻辑备份相比，物理的或“基于设备的备份”系统在复制磁盘块到备份媒介上时忽略文件结构。这样会提高备份的性能，因为备份软件在执行过程中，花费在搜索操作上的开销很少。但是，这种方法使得文件的恢复变得复杂而且缓慢。因为文件并不是连续存储在备份媒介上。为了允许文件恢复，基于设备的备份必须要收集文件和目录是如何在磁盘上组织的信息，才能使得备份媒介上的物理块与特定的文件相关联。因此，物理备份适合于指定一个特定的文件系统来实现，且不易移植。基于文件的备份方案则更易移植，因为备份文件包含的是连续文件。物理备份的另一个缺点是可能引入数据的不一致性。操作系统的核心一般会在写磁盘前对要写的数据进行缓存，而物理备份的特点是可跨越磁盘块，这样容易忽略文件缓存区中的数据，备份文件的较早版本。相对地，基于文件的备份方案考虑了文件的缓存区，备份了文件的当前版本。

2. 按备份策略，可分为完全备份、增量备份、差分备份

完全备份(Full Backup)是指对整个系统(如组成服务器的所有卷)或用户指定的所有文件进行一次完整的备份，这是最基本也是最简单的备份方式。这种备份方式的好处是很直观，容易被人理解。如果在备份间隔期间出现数据丢失等问题，可以只使用一份备份文件快速地恢复所丢失的数据。完全备份的不足之处也很明显：它需要备份所有的数据，并且每次备份的工作量也很大，需要大容量的备份媒介，如果完全备份比较频繁，在备份文件中就有大量的数据是重复的。这些重复的数据占用了大量的存储空间，这对用户来说就意味着增加成本。如果需要备份的数据量很大，备份数据时进行读写操作所需的时间也会较长。因此这种备份不能进行得太频繁，只能每隔较长一段时间才进行一次完整的备份。一旦发生数据丢失，只能使用上一次的备份数据恢复到当时的数据状况，期间更新的数据就有可能丢失。

为了解决完全备份的主要缺点，增量备份(Incremental Backup)应运而生。增量备份只备份相对与上一次备份操作以来新创建或者更新过的数据。通常特定的时间段内只有少量的文件发生改变，没有重复的备份数据，既节省了存储空间，又缩短了备份时间。因而这种备份方法比较经济，可以频繁地进行。典型的增量备份方案是在偶尔进行完全备份后，频繁地进

行增量备份。但是在增量备份系统中，一旦发生数据丢失或文件误删除操作，恢复工作会比较麻烦。因为恢复操作需要查询一系列的备份文件，从最后一次完全备份开始，将记录在一次或多次的增量备份中的改变应用到文件上，增量备份的恢复需要多份的备份文件才可以完成。在这种备份下，多次备份数据间的关系就像链条一样，一环套一环，其中任何一次备份数据出现问题都会导致整个链条脱节。因此这种备份的可靠性相对较差。

差分备份(Differential Backup)即备份上一次完全备份后产生和更新的所有新的数据。它的主要目的是将完全恢复时涉及的备份记录数量限制在 2 个，以简化恢复的复杂性。差分备份在避免另外两种备份策略缺陷的同时，又具有了它们的优点。首先，它无须频繁地做完全备份，工作量小于完全备份，因此备份所需时间短，并节省存储空间；其次，虽然每次做差分备份工作的任务比增量备份的工作量要大，但是它的灾难恢复相对简单。系统管理员只需要对两份备份文件进行恢复，即完全备份的文件和灾难发生前最后的一次差分备份文件，就可以将系统恢复。而在增量备份中，要顺序地进行从上次完全备份以来的每一次增量备份的恢复。

3. 按备份时系统的工作状态，可分为冷备份、热备份

冷备份又称离线备份，指在进行备份操作时，系统处于停机或维护状态。采用这种方式，备份的数据与系统中此时段的数据完全一致。冷备份的缺点是备份期间备份数据源不能使用。

热备份又称在线备份或同步备份，指进行备份操作时，系统处于正常运转状态下的备份。这种情况下，由于系统中的数据可能随时在更新，备份的数据相对于系统的真实数据可有一定的滞后。

14.1.5　数据存储介质

除了软磁盘和硬盘外，以下存储介质在进行大量数据备份时会经常使用到如下几种存储介质。

1. 独立磁盘冗余阵列(RAID)

RAID 在基于较好性价比的同时，提供了较好的数据保护和可靠性。尽管 RAID 比光介质存储设备和磁带昂贵，然而在任何需要容错性和快速在线数据访问的地方，它能提供最佳的数据保护。RAID 能防止由磁盘硬件故障造成的数据丢失。

2. 磁光盘机

磁光盘机(MO Drive)通常有 3.5 英寸和 5.25 英寸两种，单片 MO 容量从 230MB 到 2.6GB，甚至更高。相对普通磁带机而言，MO 采用随机存储方式，最大特点是读写速度快。此外，MO 的数据保存时间长，由于 MO 只有在极高温度下(如激光照射)才能够修改数据，并且有外壳保护，不像 CD-ROM 容易被划伤，数据可保存 20 年以上。

3. WORM

WORM(一次刻写多次读取)介质是永久备份和归档的理想工具。可擦除介质能够取代日

常备份用的磁带，在数据短期存储的情况下可以进行擦除或修改操作。目前有多种类型的 WORM 和可重写光盘可供使用。通常使用的 5.25 英寸介质每盘提供 2.6GB 的存储容量，12 英寸盘可存储 15GB 的数据。

4. 只读光盘(CD-R)或可擦除光盘(CD-RW)、DVD-R、DVD-RW

一种可用的低端光介质，包括一次刻写光盘(CD-R)和可擦除光盘(CD-RW)及只读 DVD-R、可擦写 DVD-RW。

5. 光盘库

光盘库(MO Jukebox)类似磁带库，只是采用光盘机和光盘片，是最佳的自动存储设备，成本较磁带库高。

6. 磁带

根据各种场合的需要，磁带提供了兼顾容量和性能的出色的数据备份方式。低端 Travan 级磁带介质单盒可容纳 4GB 的数据量，其传送速度为 514KB/s。高端数字线性磁带(DLT)每盒能处理 35GB 的数据量，它每秒钟提供 5MB 的数据吞吐量。在其他场合应用的是像 DAT 这样的主流磁带技术。在压缩数据模式下，所有的存储容量和数据吞吐速率都可以加倍。磁带的备份容量远大于其他方式。磁带低廉的价格使它成为替代光介质的经济方式。磁带介质同时可提供每日、每周和每月的安全离线数据存储。磁带是最佳的中长期数据保存(2~15 年)方式。

磁带可通过磁带机进行读写。磁带机是最常见的大容量备份设备，目前存在许多制式，QIC、4mm、8mm、3480/3490、DLT、DST 等，所有磁带设备都采用线性数据流存储方式。

7. 磁带库

磁带库(Tape Library)是一种自动存储设备，磁带库设备有多个磁带插槽、一个或多个磁带机和由 SCSI 指令控制的机械臂，存储量大，配合数据存储管理软件实现存储管理的自动化。

14.2　数据存储技术

存储设备与服务器的连接方式通常有三种：一是存储设备与服务器直接相连接，称为 DAS；二是存储设备直接联入现有的 TCP/IP 的网络中，称为 NAS；三是将各种存储设备集中起来形成一个存储网络，以便于对数据的集中管理，这样的网络称为 SAN。

14.2.1　DAS

DAS(Direct-Attached Storage)技术是最早被采用的存储技术，如同 PC 机的结构，是把外部的数据存储设备都直接挂在服务器内部的总线上，数据存储设备是服务器结构的一部分，但由于这种存储技术是把设备直接挂在服务器上，随着需求的不断增大，添加的设备越来越

多，导致服务器和存储独立数量较多，资源利用率低下，使得数据共享受到严重的限制。因此使用在一些小型网络应用中，DAS 连接模式示意图见图 14-4。

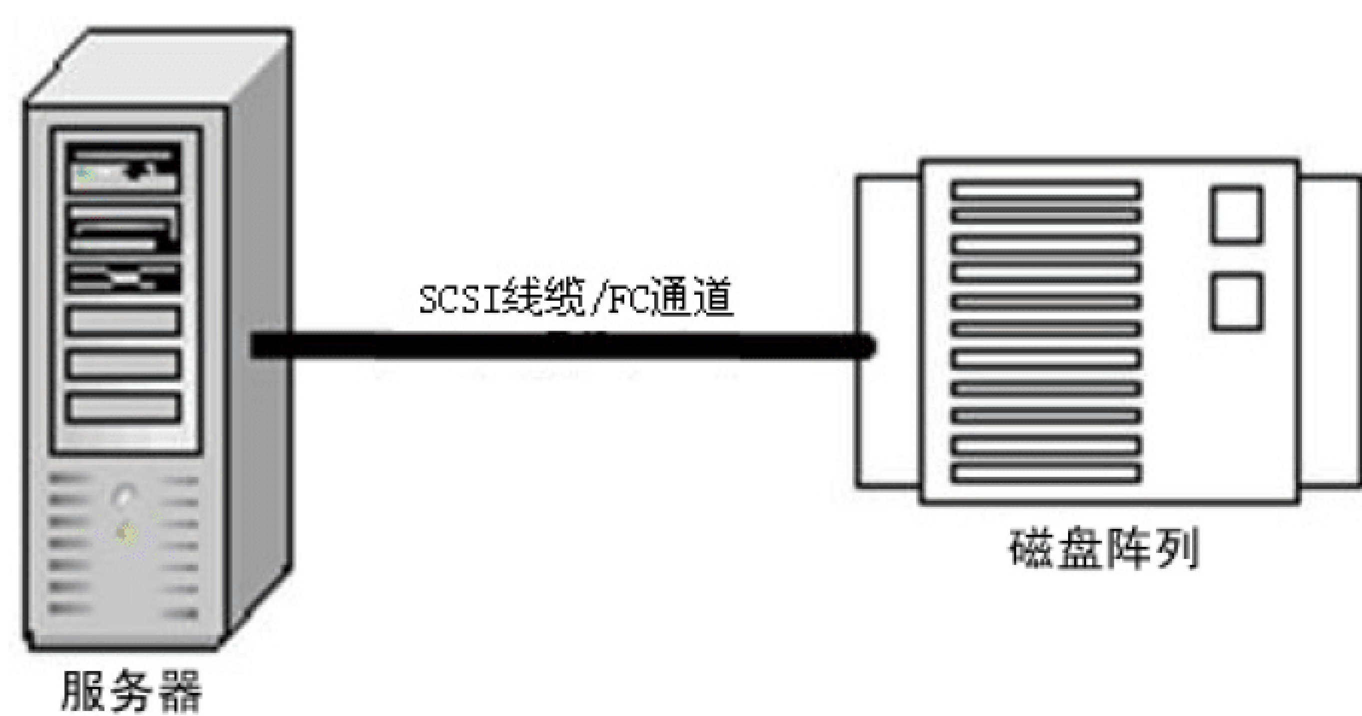


图 14-4　DAS 连接模式

14.2.2　NAS

NAS(Network-Attached Storage)改进了 DAS 技术，通过标准的网络拓扑结构，用户只需直接与企业网络连接即可使用 NAS 存储提供的服务，不依赖其他服务器。NAS 是在一个小型磁盘阵列柜的基础上，结合内置的 CPU、内存、主板，自带嵌入式操作系统，工业级的部件配合精简化的操作系统使其具备独力工作的能力。NAS 通常提供易用的操作解密，使得非计算机专业的操作人员也可轻松掌握。典型的 NAS 连接模式如图 14-5 所示。

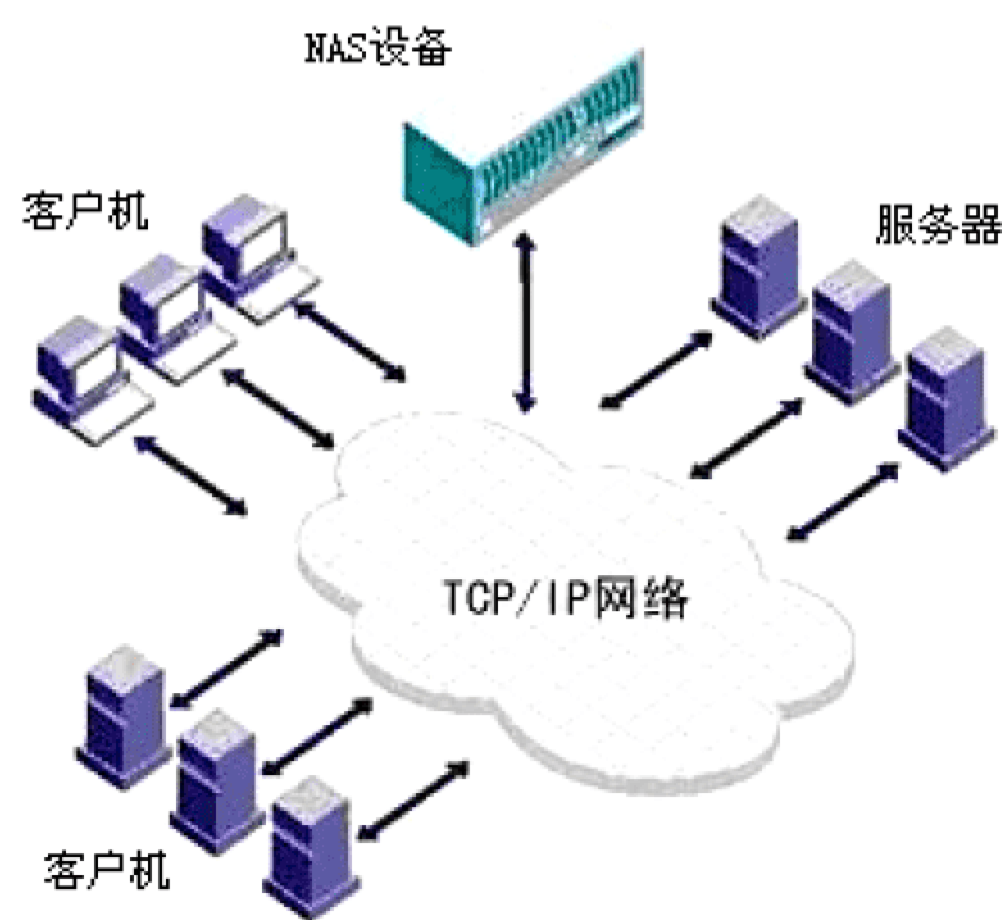


图 14-5　NAS 连接模式

14.2.3　SAN

传统 SAN(Storage Area Network)的主要支撑技术是光纤通道(Fibre Channel，FC)技术。与 NAS 完全不同，它不是把所有的存储设备集中安装在一个服务器中，而是将这些设备单独通过光纤交换机连接起来，形成一个光纤通道存储在网络中，然后再与企业的局域网进行连接，这种技术的最大特性就是将网络、设备的通信协议与存储传输介质隔离开，因此存储数据的传输不会受网络状态的影响。

基于光纤交换机的 SAN 存储，通常会综合运用链路冗余与设备冗余的方式，如图 14-6 所示，同一服务器访问磁盘阵列有多条冗余路径，不论其中的部分线路或者部分光纤交换机出现故障，都不会导致服务器访问存储失败。这种方式部署成本较高，但对银行、证券、数

据中心等存储了大量关键数据，且不允许业务中断的行业来说非常重要。

目前处于迅速成长期的 IP SAN 存储，是在传统的 SAN(FC SAN)的基础上演变而来的。IP SAN 是在以太网上架构一个 SAN 存储网络，把服务器或普通工作站与存储设备连接起来的存储技术。IP SAN 在 FC SAN 的基础上更进一步，它把 SCSI 协议完全封装在 IP 协议之中。简单来说，IP SAN 就是把 FC SAN 中光纤通道解决的问题通过更为成熟的以太网实现，从逻辑上讲，它是提供区块级服务的彻底的 SAN 架构。

IP SAN 的主要优点是：能节约大量成本、加快实施速度、优化可靠性以及增强扩展能力等。采用 iSCSI 技术组成的 IP SAN 可以提供和传统 FC SAN 相媲美的存储解决方案，而且普通服务器或 PC 机只需要具备网卡，即可共享和使用大容量的存储空间。与传统的分散式直连存储方式不同，它采用集中的存储方式，极大地提高了存储空间的利用率，方便了用户的维护管理。

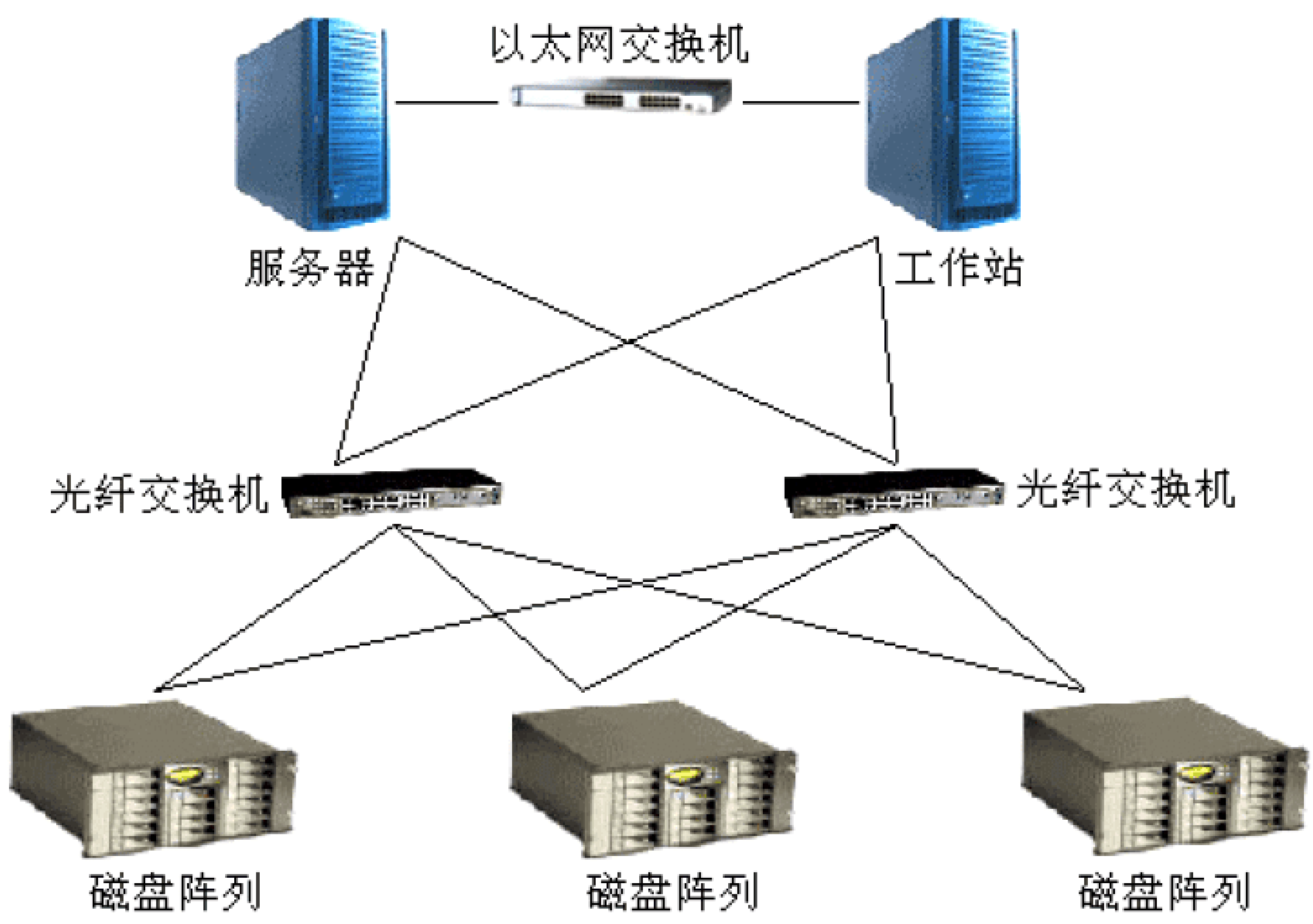


图 14-6　SAN 连接模式

14.3　远程数据备份

远程数据复制技术是远程容灾系统的核心技术，在保持两地间数据一致性和实现灾难恢复中起到关键作用。数据复制的主要目的是提高分布式系统的可用性及访问性能。目前数据复制的主要方式有同步数据复制和异步数据复制两种。

14.3.1　同步数据复制

同步数据复制(Synchronous Data Replication)又称实时数据复制，是指对业务数据进行实时复制，数据源和备份中心之间的数据互为镜像，保持完全一致。这种方式实时性强，灾难发生时远端数据与本地数据完全相同，可以达到数据的零丢失，保证高度的完整性和一致性。

同步数据复制方式中，复制数据在任何时间和任何节点均保持一致。如果复制环境中任何一个节点数据发生了更新操作，这种变化会立刻反映到其他所有节点。为了保证系统性能和实用性，数据被复制在多个节点，同步复制在所有节点通过更新事务保证所有备份一致。

同步复制在没有并发事务发生时连续执行，但减少了更新执行，增加了事务响应时间，因为事务附加了额外的更新操作和消息发送。

同步数据复制方式的工作流程如图 14-7 所示，其中 1、2、3、4 个步骤阐述了数据在生产中心与灾难备份中心间的流动过程。

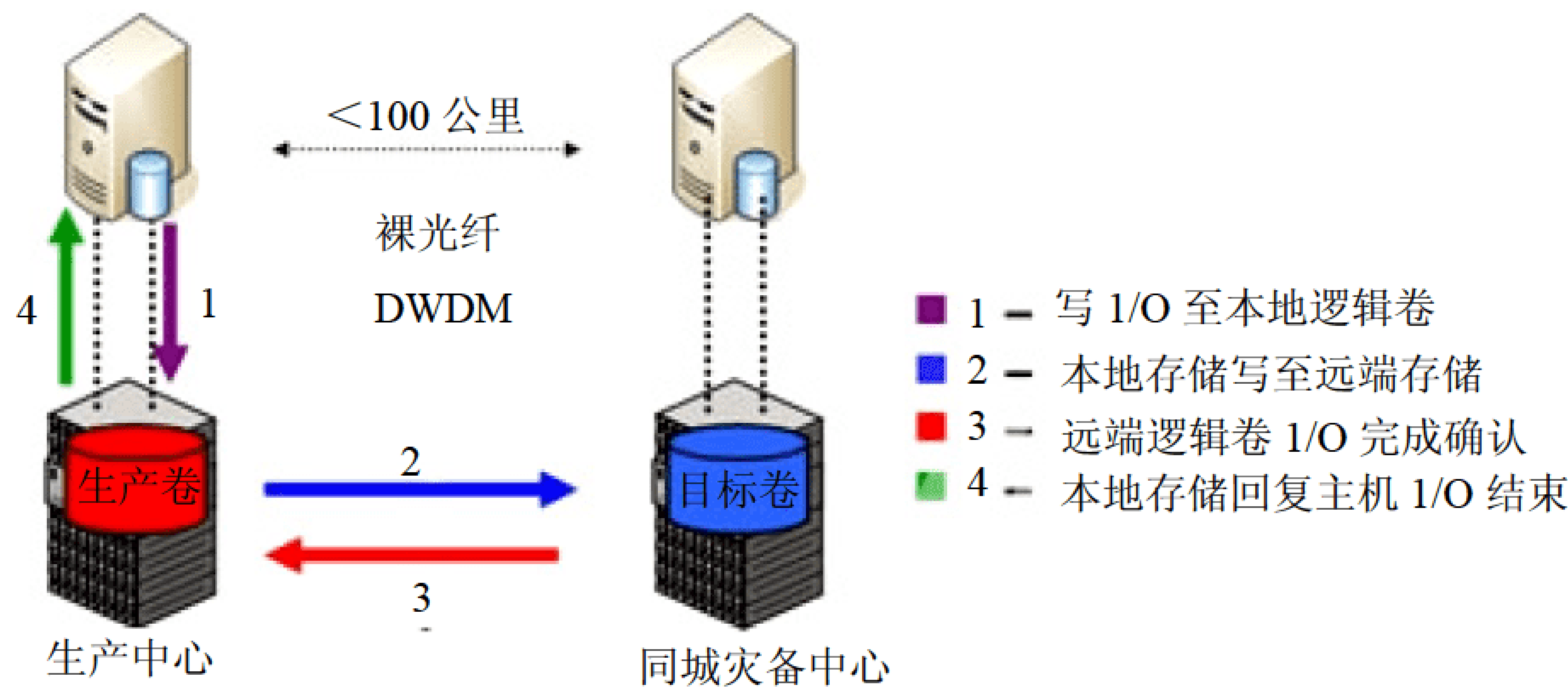


图 14-7　同步数据复制工作流程

14.3.2　异步数据复制

异步数据复制(Asynchronous Data Replication)是将本地的数据通过后台同步的方式复制到异地。这种方式可能有分钟级的短时数据丢失，很难达到零数据丢失。异步复制的原理是对本地主卷写完成后，不必等待远程二级卷的写完成，主机立即可处理下一个 I/O。因此，对本地主机性能影响很小。

与同步数据复制方式相比，异步数据复制方式对带宽和距离的要求低很多，它只要求在某个时间段内能将数据全部复制到异地即可，同时异步数据复制方式也不会明显影响应用系统的性能。从传输距离上说，异步数据复制可以使用信道扩展器或其他技术，使传输距离延长，能够达到几千公里。其缺点是在本地生产数据发生灾难时，异地系统上的数据可能会短暂损失(如果广域网速率较低，交易未完整发送的话)，但不影响一致性(类似本地数据库主机的异常关机)。

异步数据复制结合同步数据复制的应用示意图见图 14-8 中应用综合了两种数据复制方式的特点，既实现了数据的零丢失，又达到异地容灾的目的。

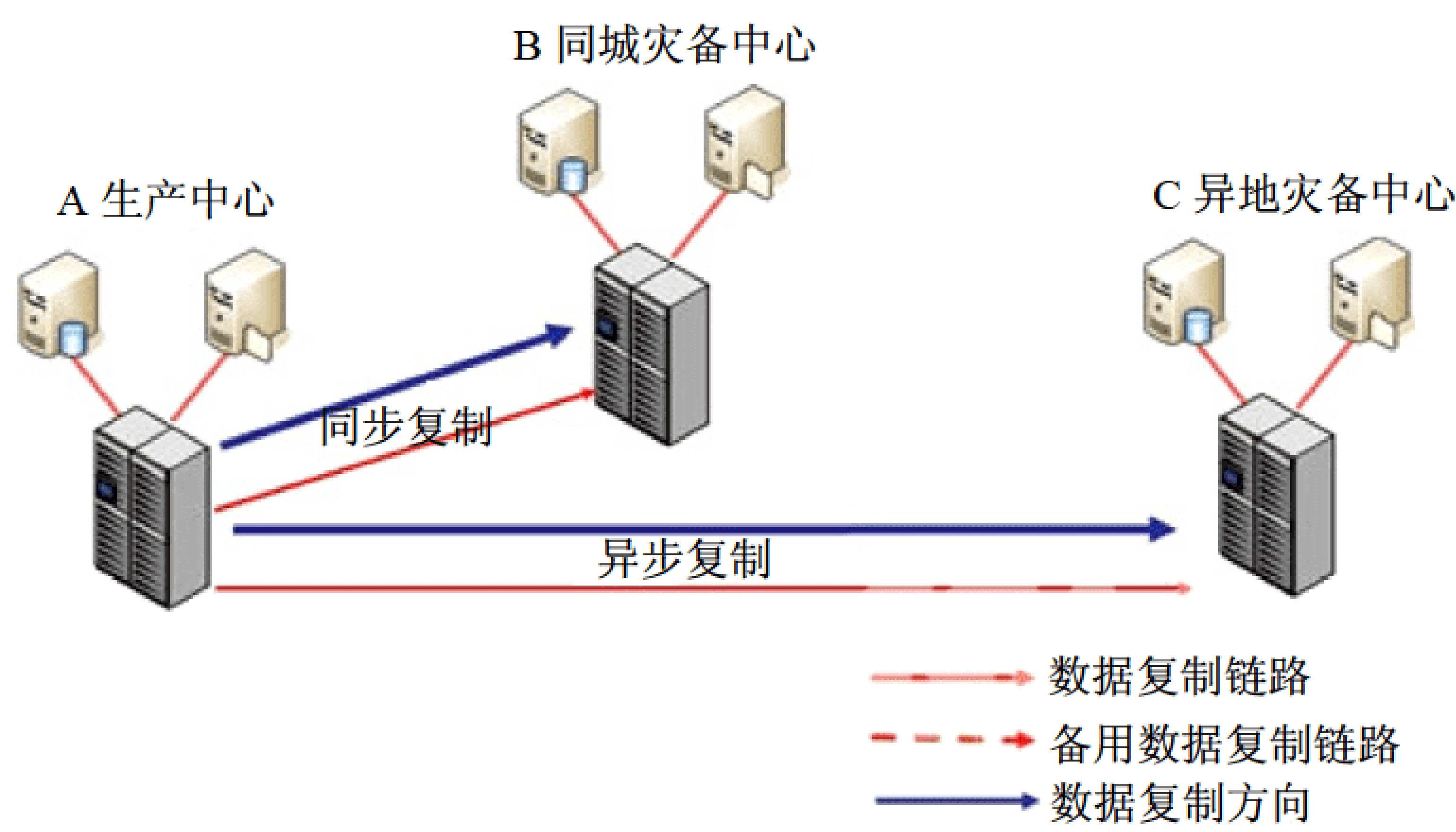


图 14-8　同步数据复制工作流程

14.4　个人数据备份

相比服务器数据备份，个人计算机数据备份原理、操作都要简单一些，下面介绍两种典型的个人计算机数据备份方式。

14.4.1　Windows 自带的备份功能

Windows 系列操作系统中，Windows 2000 及其之后的系统，如 Windows XP、Windows Server 2003、Windows 7、Windows Server 2008 等，都内置了数据备份功能。当没有专业数据备份软件可用时，使用 Windows 自带的备份工具也能在一定程度上起到数据保护的作用。Windows 自带的备份工具使用比较简单，分为以下几个步骤。

(1) 单击“开始”按钮，选择菜单“程序”→“附件”→“系统工具”→“备份”，出现图 14-9 所示的界面。

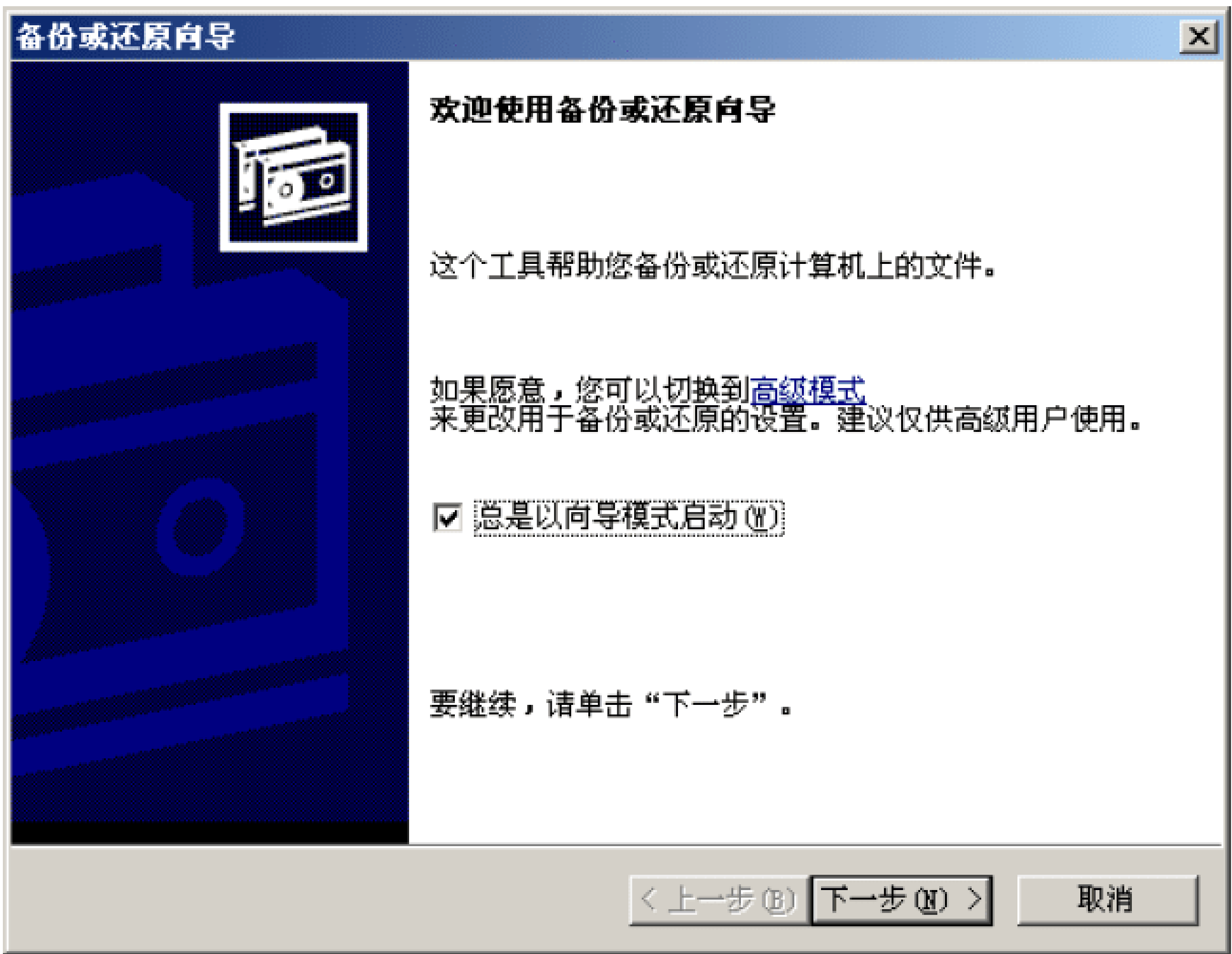


图 14-9　Windows 自带备份向导

(2) 单击“下一步”按钮后，界面会提示当前操作是要进行数据备份，还是数据恢复，这里我们以选择数据备份为例，继续单击“下一步”按钮，则出现如图 14-10 所示的选择界面。

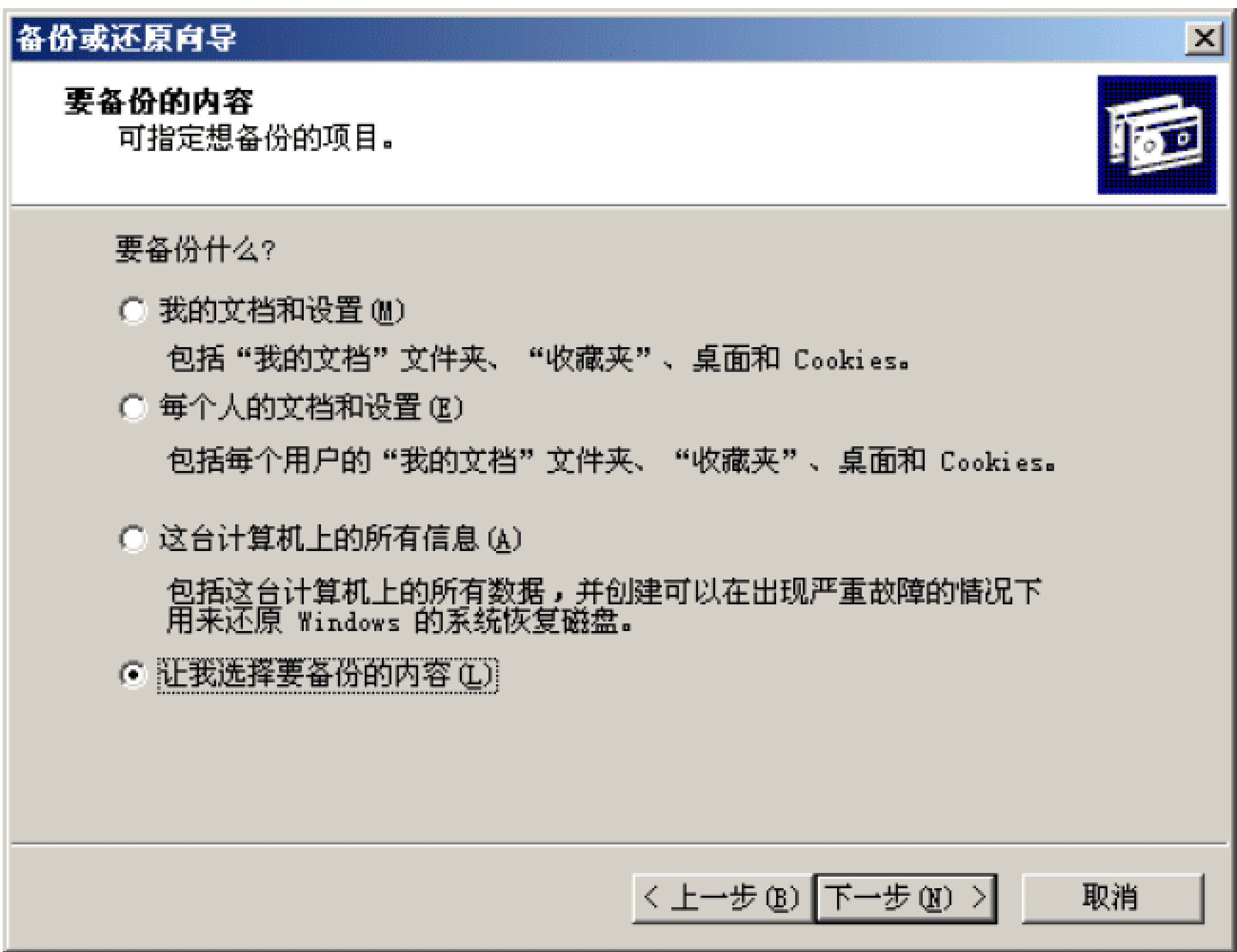


图 14-10　选择备份数据来源

本例中，我们选择“让我选择要备份的内容”，即自行选择备份哪些数据。然后单击“下一步”按钮，则出现如图 14-11 所示的选择要备份的数据项的界面。这里我们选择备份“C: ”盘下的“boot”目录(即文件夹)，单击“下一步”按钮。

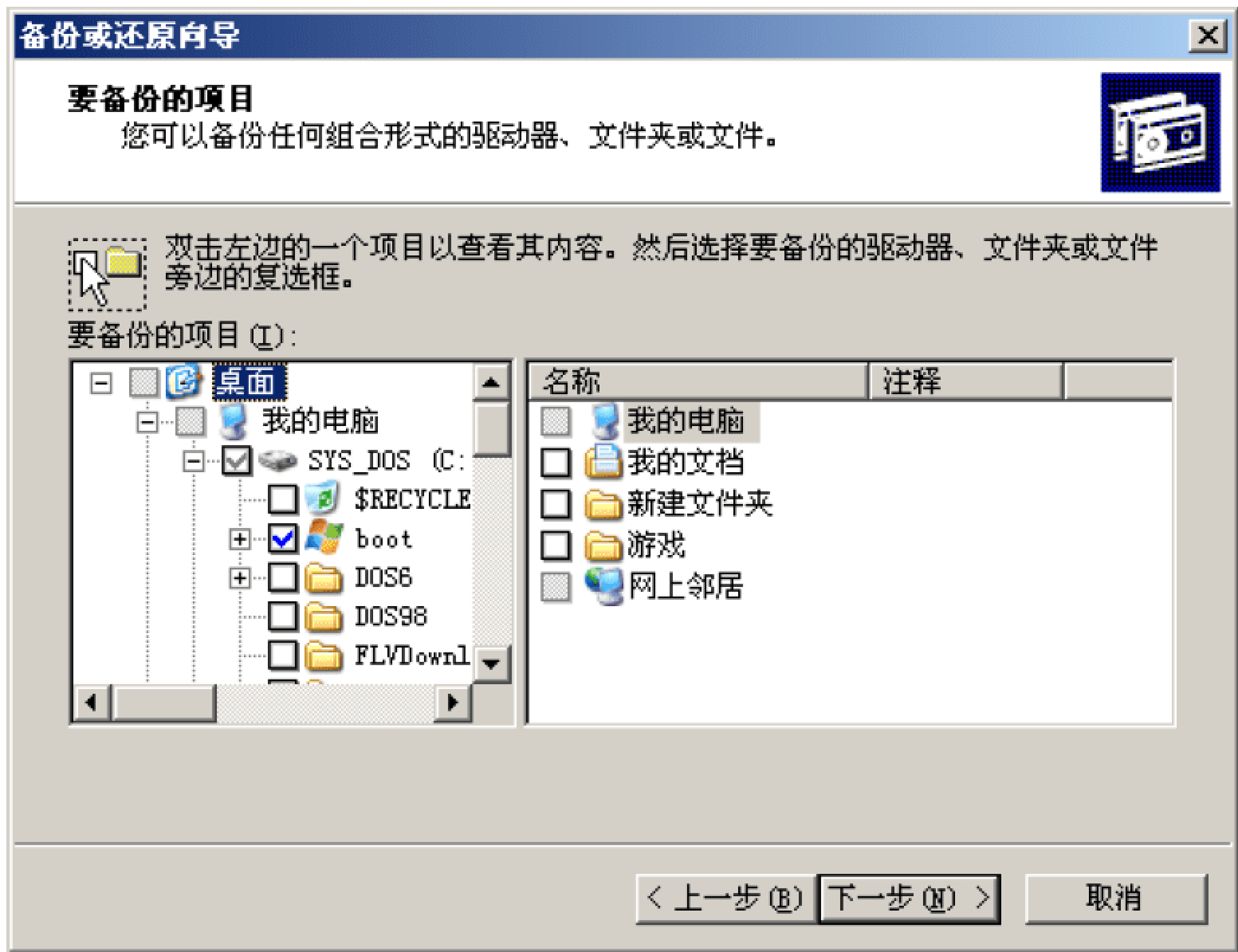


图 14-11　选择备份数据项

(3) 在弹出的界面中要求输入备份数据的存放位置及备份文件的文件名，这里我们选择备份到“V:”盘，备份文件名称是“Backup”，如图 14-12 所示。

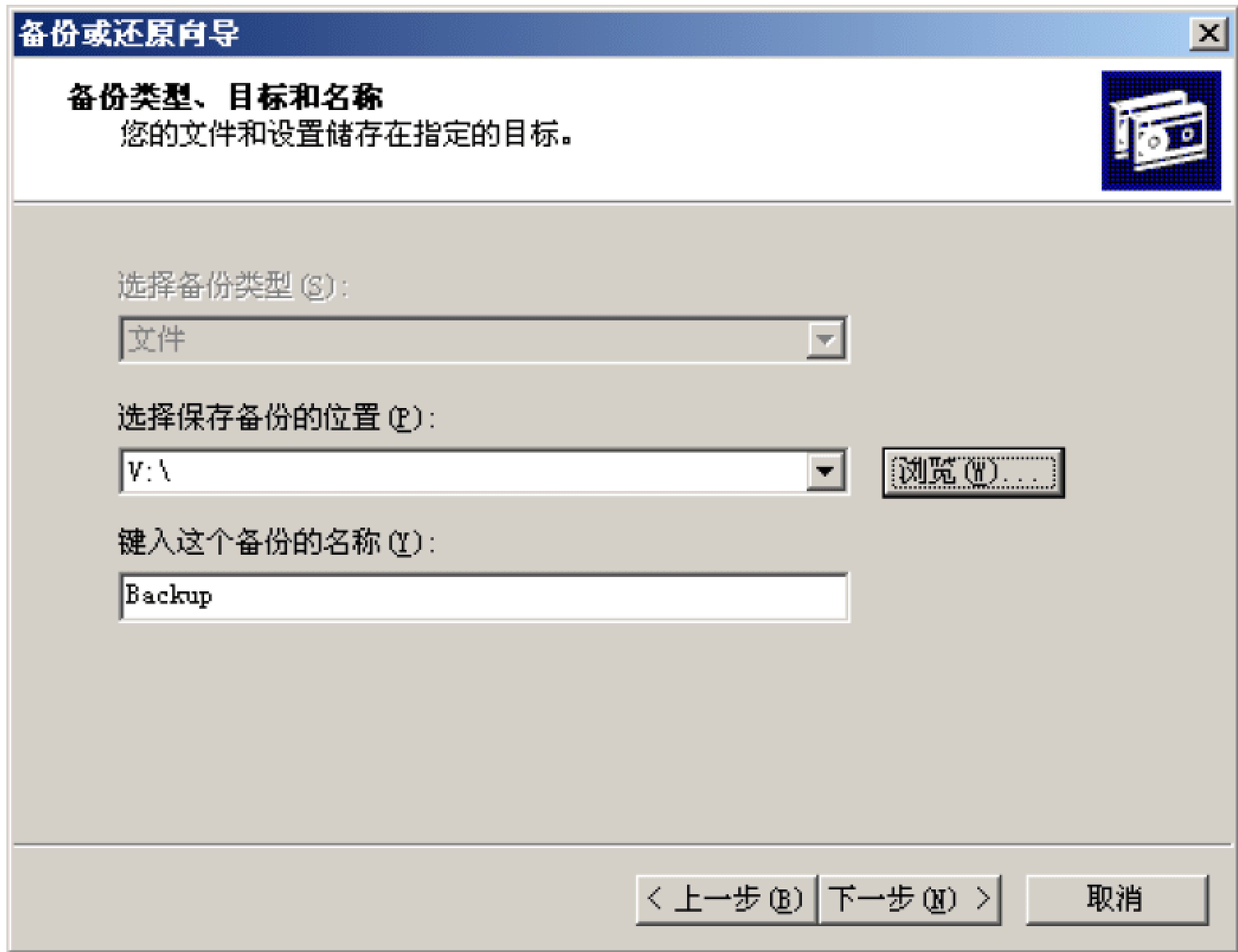


图 14-12　选择备份数据项

(4) 继续单击“下一步”按钮，出现确认备份界面，在此界面中单击“完成”按钮，系统即开始备份数据，备份过程如图 14-13 所示。

备份操作结束后，会在“V:”盘根目录产生一个名为“Backup.bkf”的文件，此文件包含的就是备份数据源“C:\boot”的所有数据。

Windows 自带的数据备份工具的操作比较简单，按照其向导程序一步一步进行即可。其备份数据的恢复操作也可用类似方法完成。



图 14-13　数据备份过程

14.4.2　Symantec Ghost 备份功能

Symantec Ghost(通常简称 Ghost)是一款强大、易用、专业的备份工具，它可针对整个磁盘进行备份/恢复，也可针对磁盘上的特定分区进行备份/恢复。Ghost 还支持强大的网络备份/恢复，可通过网络进行主机间一对一、一对多的数据备份/恢复操作，在管理包含众多主机的 PC 机房时，通过网络进行批量主机操作系统备份、恢复非常方便。下面以用 Ghost 11.0.2 实现磁盘分区备份为例，来说明 Ghost 的基本用法。

启动 Ghost 后，选择菜单 Local→Partition→To Image，即将本地磁盘的分区备份到映像文件(Image)，如图 14-14 所示。

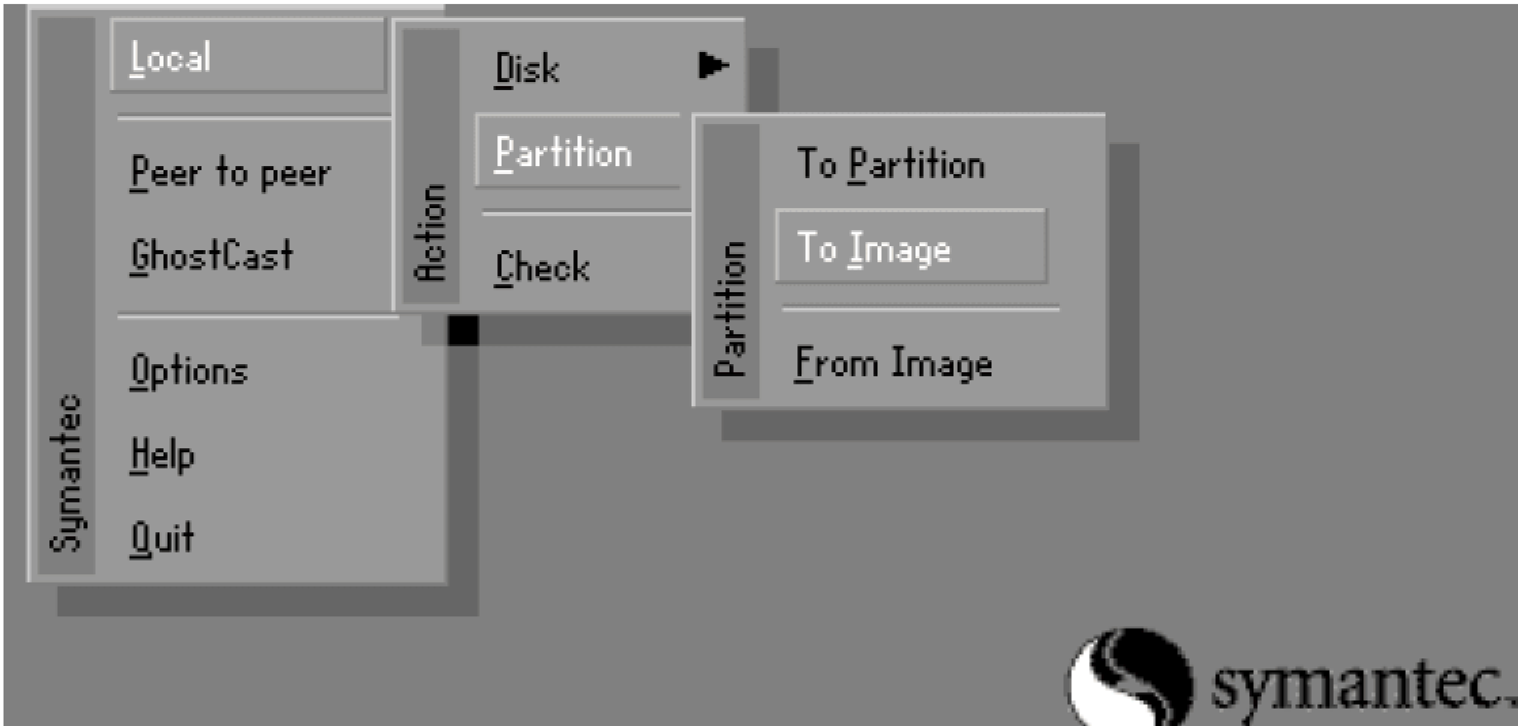


图 14-14　在 Ghost 中选择备份本地磁盘的分区到映像文件

在后续界面中，需要选择备份数据的来源磁盘(见图 14-15 中的 Select local source drive)，本例中我们选择 238GB 的那个磁盘，单击“OK”按钮。

接下来选择需要备份的分区，即备份来源磁盘的哪个分区，选择界面见图 14-16。

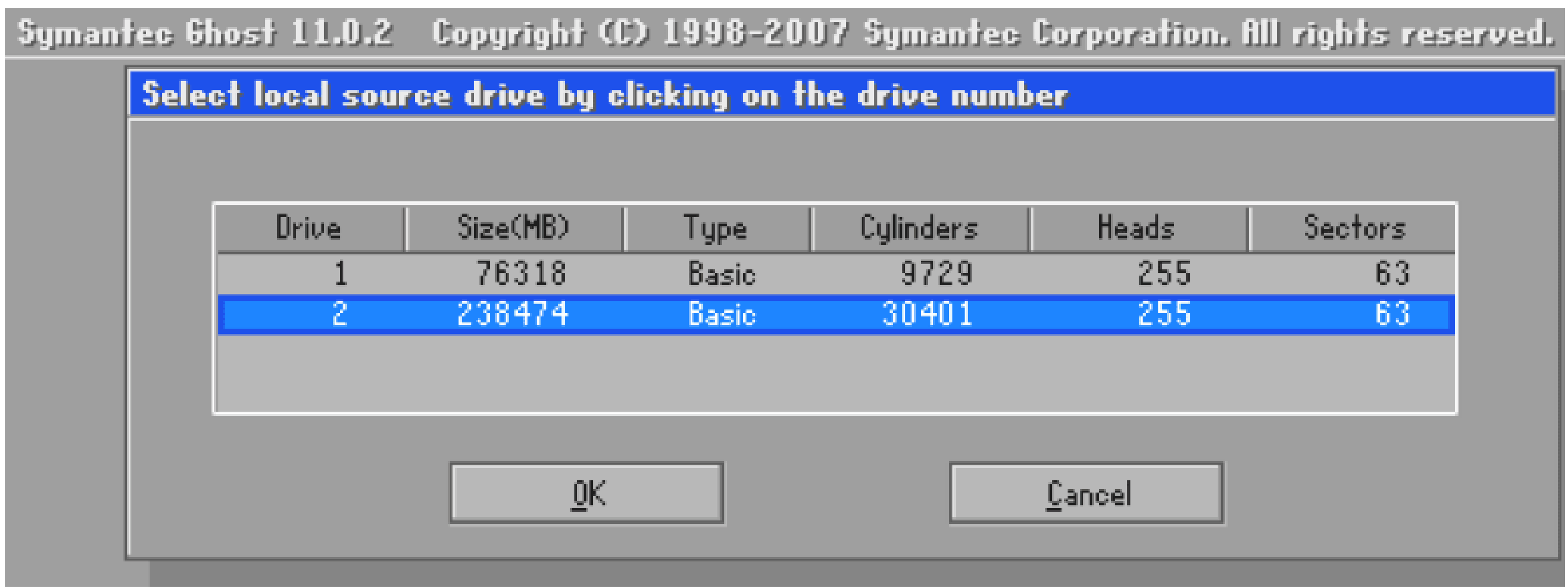


图 14-15　在 Ghost 中选择备份源磁盘

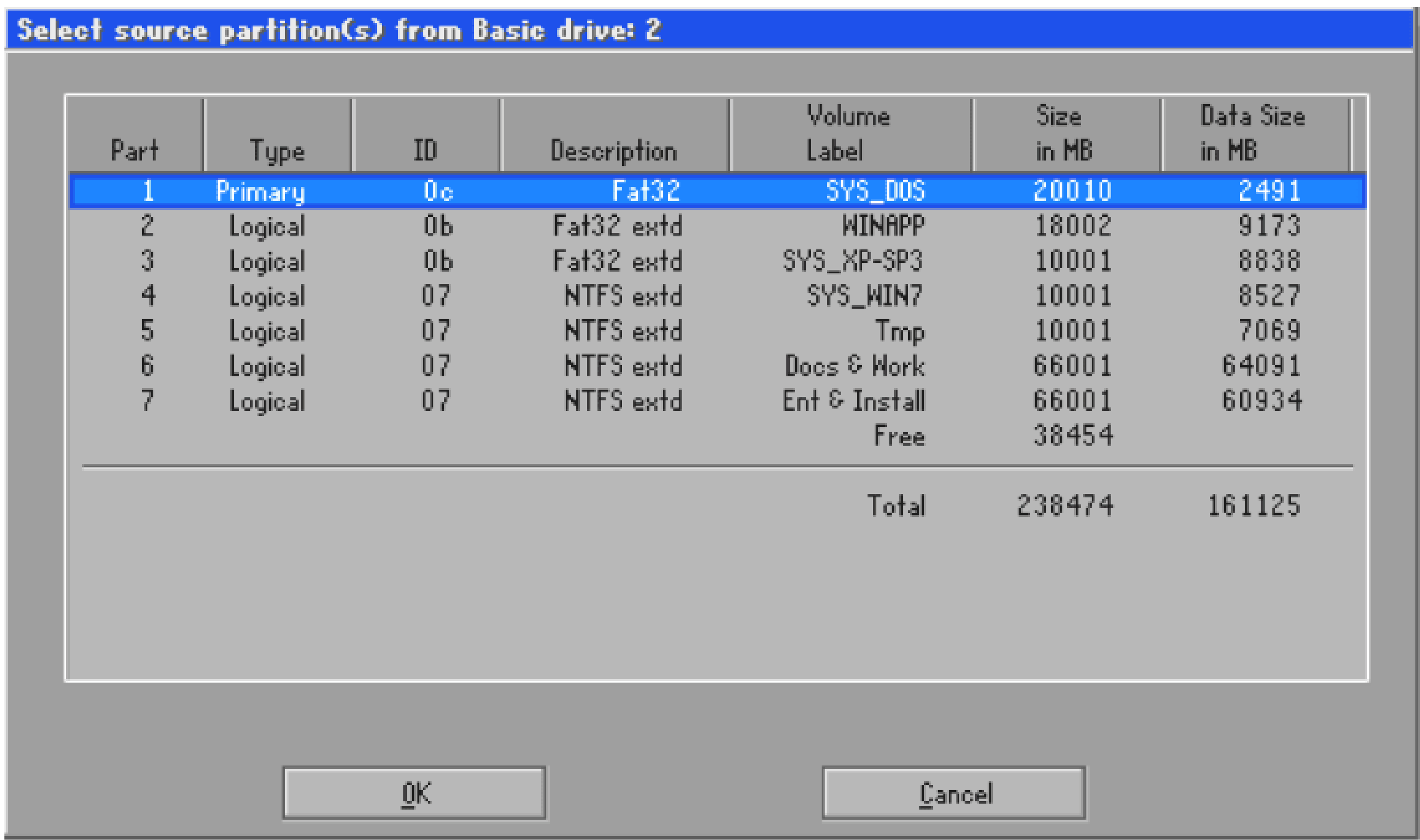


图 14-16　在 Ghost 中选择备份源分区

图 14-16 中，我们选择备份该盘的第一个分区，其卷标为“SYS_DOS”，容量为 20 010MB，单击 OK 按钮后，则弹出备份文件存放路径、存储文件名的界面，如图 14-17 所示，这里我们选择的路径是“T:\”，备份数据的文件名(File Name)是“SYSC”，单击 Save 按钮。

在接下来弹出的界面中，需要选择数据备份文件的压缩方式，有三个选项 No(不压缩)、Fast(快速压缩)、High(最大压缩)，压缩比越高，需要的备份数据的时间也就越长，这里根据用户自己的需要进行选择。

选好压缩方式后，最后一个确认开始备份的界面，选择 Yes 开始备份，选择 No 则取消备份。最后这一步操作是很重要的一个环节，操作错误，会导致大量数据丢失。当把一个分区备份为一个映像文件时通常没有什么风险，但如果是把一个分区备份或复制到另外一个分区，或者将一个备份数据文件恢复到某个分区，就需要格外小心。如果错误地选择了数据复制、恢复的目标分区，则会导致该目标分区的数据被覆盖，并且覆盖后该分区的数据很难挽回。

因此，在使用 Ghost 进行数据复制、恢复操作时，在最后一步确认界面，一定要仔细看清楚，当前 Ghost 操作的目标。图 14-18 是截取的确认界面中的详细信息(Details)栏目的内容，看清楚此栏内容，确认操作目标无误，方可单击 Yes 按钮进行数据复制、恢复操作。

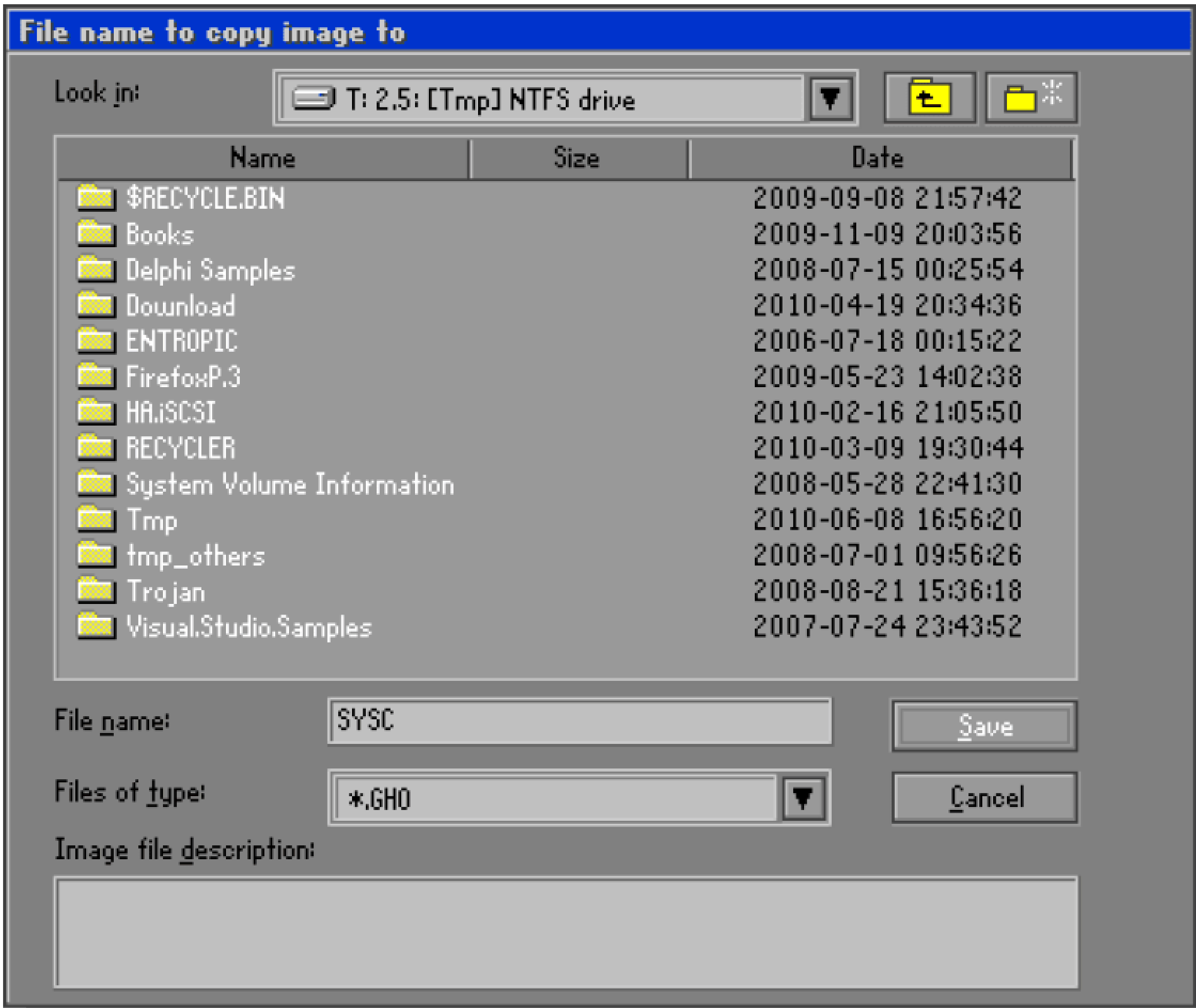


图 14-17　在 Ghost 中选择备份文件存放路径、文件名

如图 14-18 所示，本例中备份数据源(Source Partition)是容量 20 010MB，卷标为“SYS_DOS”的分区，和前面操作的选择一致。备份数据的目标文件(Destination File)是“T:\SYSC.GHO”，也与前述操作一致，因此可以开始备份操作。



图 14-18　确认 Ghost 操作的目的位置

若数据备份/恢复的目的位置不是文件，而是分区，或者另一个磁盘，则需要仔细核对，通过目的对象的卷标、容量等信息，检查是否正确地选择了将进行操作的目的对象。

应用 Ghost 进行数据恢复操作时，步骤与备份操作类似，但是需要特别小心，不能弄错了数据恢复的目的地，否则很容易导致不可挽回的数据丢失。

本 章 小 结

本章从信息安全的基本要素“数据完整性”入手，介绍了数据完整性的基本概念、重要意义及与数据保密性的辨析。介绍了数据备份的几种典型分类和常用存储介质。在阐述当前主流的 DAS、NAS、SAN 存储技术的基本结构后，引入了同步数据复制、异步数据复制的概念。最后介绍的 Windows 自带备份工具以及 Symantec Ghost，都是针对个人计算机用户的数据备份手段，日常不接触服务器等设备的用户能从此中受益。

课 后 练 习

一、填空题

1. 通常说的磁盘阵列 RAID，其缩写来自于(　　　　　　)。
2. 按备份策略划分，数据备份可分为完全备份、增量备份、(　　　　　　)。
3. 增量备份只备份相对与上一次备份操作以来(　　　　　　)的数据。
4. DAS、NAS 存储方式中，需要用到网络的是(　　　　　　)。
5. 基于光纤交换机的 SAN 存储，通常会综合运用(　　　　　　)冗余与(　　　　　　)冗余的方式。

二、选择题

1. 数据在传输过程中，被攻击者截获并读取内容，破坏的是数据的(　　)。
   A. 保密性　B. 完整性　C. 可用性　D. 不可抵赖性
2. 数据在传输过程中，被攻击者修改了部分内容，破坏的是数据的(　　)。
   A. 保密性　B. 完整性　C. 可用性　D. 不可抵赖性
3. 至少需要 3 块硬盘组 RAID，且其中只有一块硬盘损坏时，不会造成数据丢失的 RAID 方式是(　　)。
   A. RAID 0　B. RAID 1　C. RAID 5　D. RAID 10
4. 存储技术中所说的 DAS，其缩写来自于(　　)。
   A. Disk Access System　B. Disk Access Storage
   C. Direct Attached System　D. Direct Attached Storage
5. Symantec Ghost 可以备份独立的(　　)。
   A. 分区、磁盘　B. 分区、文件
   C. 磁盘、文件　D. 分区、磁盘、文件

三、简答题

1. 数据保密性与数据完整性的主要区别是什么？
2. 保护数据完整性的主要手段是什么？
3. FC-SAN 与 IP-SAN 的主要优点、缺点是什么？
4. 同步数据复制与异步数据复制的各自特点是什么？
5. Symantec Ghost 主要适用于哪些应用场合的数据备份？

第15章　信息安全评测与风险评估

信息安全风险是人为或自然的威胁利用系统存在的脆弱性引发的安全事件，并由于受损信息资产的重要性而对机构造成的影响。通过风险评估，能及早发现和解决问题，防患于未然。

本章结合国内外信息安全风险评估发展的现状，给出了有关信息安全评估的主要概念、基本步骤、实施流程和评估分类等内容，并对风险评估的作用和相关标准等方面进行了阐述，旨在使信息安全风险评估作为科学的方法真正能够为读者接受、理解和运用。

本章重点

- 概述
- 信息安全风险评估
- 信息安全风险评估标准

15.1　概　　述

信息安全风险评估，是指依据国家风险评估有关管理要求和技术标准，对信息系统及由其存储、处理和传输的信息的机密性、完整性和可用性等安全属性进行科学、公正的综合评价的过程。通过对信息及信息系统的重要性、面临的威胁、其自身的脆弱性以及已采取安全措施有效性的分析，判断脆弱性被威胁源利用后可能发生的安全事件以及其所造成的负面影响程度来识别信息安全的安全风险。

15.2　信息安全风险评估

信息安全风险评估是信息安全保障体系建立过程中的重要评价方法和决策机制。没有准确及时的风险评估，将使得各个机构无法对其信息安全的状况做出准确的判断。因为任何信息系统都会有安全风险，信息安全建设的宗旨之一，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，使残余风险降低到可接受的范围内。

风险评估是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

15.2.1　评估概述

评估是一个收集安全保障证据的过程，也是针对功能性和保障性准则的分析过程。通过评估，可以得到可信度的某种度量，指示系统满足具体标准的程度。评估时所采用的标准依赖于评估的目标以及所采用的评估方法。

信息安全风险评估是建立信息安全保障机制中的一种科学方法。对信息系统而言，存在风险并不意味着不安全，只要风险控制在可接受的范围内，就可以达到系统稳定运行的目的。风险评估的结果为保障信息系统的安全建设、稳定运行提供了技术参考。在规划与设计阶段，风险评估的结果是安全需求的来源，为信息系统的安全建设提供依据；在系统运行维护阶段，由于信息系统的动态性，需要定期地进行风险评估，以了解、掌握系统安全状态，风险评估是保证系统安全的动态措施。同时，风险评估是信息系统安全等级确定及建设过程中一种不可或缺的技术手段。

风险评估包括的主要任务如下。

- 识别组织面临的各种风险。
- 评估风险概率和可能带来的负面影响。
- 确定组织承受风险的能力。
- 确定风险消减和控制的优先等级。
- 推荐风险消减对策。

通常信息安全系统的评估方法具有以下几个特征。

- 一组功能需求，定义了系统或者产品的安全功能。
- 一组安全保障需求，描述系统或者产品为满足功能需求而采取的若干措施，这种措施通常指所需的安全保障证据。
- 一种用于确定系统是否满足功能需求的方法，这种方法建立在分析安全保障证据的基础之上。
- 一种针对评估结果的度量标准(称为可信等级)，它是为产品或者系统定义的关于安全功能的需求，表明产品或者系统的可信程度。

15.2.2　评估步骤

在风险评估过程中，有几个关键的问题需要考虑。

- 首先要确定保护的对象(或者资产)是什么？它的直接和间接价值如何？
- 其次资产面临哪些潜在威胁？导致威胁的问题所在？威胁发生的可能性有多大？
- 资产中存在哪些弱点可能会被威胁利用？利用的容易程度又如何？
- 一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？
- 最后，组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？

解决以上问题的过程，就是风险评估的过程。

在风险评估过程中，可以采用多种操作方法，包括基于知识(Knowledge-based)的分析方法、基于模型(Model-based)的分析方法、定性(Qualitative)分析和定量(Quantitative)分析，无论是何种方法，共同的目标都是找出组织信息资产面临的风险及其影响，以及目前安全水平与

组织安全需求之间的差距。

15.2.3　评估分类

在风险管理的前期准备阶段，组织已经根据安全目标确定了自己的安全战略，其中就包括对风险评估战略的考虑。所谓风险评估战略，其实就是进行风险评估的途径，也就是规定风险评估应该延续的操作过程和方式。

风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务。影响风险评估进展的某些因素，包括评估时间、力度、展开幅度和深度，都应与组织的环境和安全要求相符合。组织应该针对不同的情况来选择恰当的风险评估途径。目前，实际工作中经常使用的风险评估途径包括基线评估、详细评估和组合评估三种。

1. 基线评估

如果组织的商业运作不是很复杂，并且组织对信息处理和网络的依赖程度不是很高，或者组织信息系统多采用普遍且标准化的模式，基线风险评估(Baseline Risk Assessment)就可以直接而简单地实现基本的安全水平，并且满足组织及其商业环境的所有要求。

采用基线风险评估，组织根据自己的实际情况(所在行业、业务环境与性质等)，对信息系统进行安全基线检查(拿现有的安全措施与安全基线规定的措施进行比较，找出其中的差距)，得出基本的安全需求，通过选择并实施标准的安全措施来消减和控制风险。所谓的安全基线，是在诸多标准规范中规定的一组安全控制措施或者惯例，这些措施和惯例适用于特定环境下的所有系统，可以满足基本的安全需求，能使系统达到一定的安全防护水平。组织可以根据以下资源来选择安全基线。

- 国际标准和国家标准，例如 BS 7799-1、ISO 13335-4。
- 行业标准或推荐，例如德国联邦安全局 IT 基线保护手册。
- 来自其他有类似商务目标和规模的组织的惯例。

当然，如果环境和商务目标较为典型，组织也可以自行建立基线。

基线评估的优点是需要的资源少，周期短，操作简单，对于环境相似且安全需求相当的诸多组织，基线评估显然是最经济有效的风险评估途径。当然，基线评估也有其难以避免的缺点，比如基线水平的高低难以设定，如果过高，可能导致资源浪费和限制过度；如果过低，可能难以达到充分的安全，此外，在管理安全相关的变化方面，基线评估比较困难。

基线评估的目标是建立一套满足信息安全基本目标的最小的对策集合，它可以在全组织范围内实行，如果有特殊需要，应该在此基础上，对特定系统进行更详细的评估。

2. 详细评估

详细风险评估要求对资产进行详细识别和评价，对可能引起风险的威胁和弱点水平进行评估，根据风险评估的结果来识别和选择安全措施。这种评估途径集中体现了风险管理的思想，即识别资产的风险并将风险降低到可接受的水平，以此证明管理者所采用的安全控制措施是恰当的。

详细评估的优点如下。

- 组织可以通过详细的风险评估而对信息安全风险有一个精确的认识，并且准确定义出组织目前的安全水平和安全需求。
- 详细评估的结果可用来管理安全变化。当然，详细的风险评估可能是非常耗费资源的过程，包括时间、精力和技术，因此，组织应该仔细设定待评估的信息系统范围，明确商务环境、操作和信息资产的边界。

3. 组合评估

基线风险评估耗费资源少、周期短、操作简单，但不够准确，适合一般环境的评估；详细风险评估准确而细致，但耗费资源较多，适合严格限定边界的较小范围内的评估。在实践当中，组织多是采用二者结合的组合评估方式。

为了决定选择哪种风险评估途径，组织首先对所有的系统进行一次初步的高级风险评估，应着眼于信息系统的商务价值和可能面临的风险，识别出组织内具有高风险的或者对其商务运作极为关键的信息资产(或系统)，这些资产或系统应该划入详细风险评估的范围，而其他系统则可以通过基线风险评估直接选择安全措施。

这种评估途径将基线和详细风险评估的优势结合起来，既节省了评估所耗费的资源，又能确保获得一个全面系统的评估结果，而且，组织的资源和资金能够应用到最能发挥作用的地方，具有高风险的信息系统能够被预先关注。当然，组合评估也有缺点：如果初步的高级风险评估不够准确，某些本来需要详细评估的系统也许会被忽略，最终导致结果失准。

15.3　信息安全风险评估标准

在前面的第 2 章我们已经回顾过安全评估标准的发展历程以及各个标准相互的关系，包括：著名的《可信计算机系统评价准则》(TCSEC，又称橘皮书)，欧共体发布的《信息技术安全评价准则》(ITSEC)，加拿大发布的《加拿大可信计算机产品评价准则》(CTCPEC)，在 TCSEC 和 ITSEC 的基础上改进过的《信息技术安全评价联邦准则》(FC)，以及来自欧美七方六国的组织共同起草的《通用准则》(CC)。

上述的各种标准中有若干评估标准对整个信息安全形式化评估方法具有重大的影响力，其中最主要的有《可信计算机系统评估准则》TCSEC 和《信息技术安全评估标准》ITSEC。现在，《通用准则》CC 已经取代了这些标准而成为国际标准的评估方法。本节将以国际上的这些标准为例，介绍标准内容；结合中国的信息安全现状，介绍相关的计算机信息系统安全保护等级标准。

15.3.1　评估前的决策

即使不对系统进行安全评估，安全功能需求和安全保障需求也能提供一种良好的总体描述，体现提高保障性所需考虑的因素。对于任何系统来说，这些因素都具有十分重要的价值。在决定进行正式的评估之前，必须综合考虑安全和成本两方面的因素，例如系统的描述和特

点等因素。寻求形式化评估的组织不仅要支付评估者相应的费用，而且要承担经验丰富的专家人员的费用，以及开发安全文档和收集保障证据所需要的费用。与评估人员就培训、澄清和更正一些主要问题所进行的交互，将花费一定的开发人员的时间，甚至影响到开发和发布的进度。令人遗憾的是，即使进行了安全评估之后，系统也不能证明具有完全抵御任何攻击的能力。现实的情况是，大多数系统都进行在恶意环境中，因而系统必须能够抵御攻击和疏忽所带来的错误。

由专家独立进行的评估，专门针对安全机制的效率以及安全机制实施和运转的正确性，对于寻找产品或系统中的缺陷和弱点将起到十分重要的作用。这种系统分析的第一步是评价需求，需求必须是一致的、完整的、技术合理并且充分的，这样才能确保系统能够抵御各种威胁。系统评估的另一部分工作是分析安全特征满足安全需求的程度。评估程序需要指明管理类型，用户、安装以及其他系统，它们为管理者和维护者提供正确配置管理系统所需要的信息文档，以便安全机制能够正常工作。

下面我们介绍一些国际上主流的几种信息安全评估标准及其安全等级划分。

15.3.2　TCSEC

TCSEC，俗称橘皮书，即美国国防部的《可信计算机系统评价准则》，是第一个正式的计算机信息安全评估标准，具有划时代的意义，于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 将安全分为 4 个方面：安全策略、可说明性、安全保障和文档。该标准将计算机系统的安全划分为 4 个类别，8 个级别，按照安全程度由低到高依次是：D1、C1、C2、B1、B2、B3、A1 及超 A1 级。TCSEC 标准如表 15-1 所示。

表 15-1　TCSEC 安全评价标准

类　别	级　别	特　性	主 要 功 能
D	D1	低级保护	保护措施很少，没有安全功能
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识安全保护	强制存取控制，安全标识
	B2	结构保护	面向安全的体系结构，具有较好抗渗透能力
	B3	安全域	存取监控，具有高抗渗透能力
A	A1	验证设计	形式化的最高级描述，验证和隐蔽通道
	超 A1 级	验证源码	在 A1 安全级别基础上，增加源码级验证

1. D 类安全等级

D 类安全是最低的安全类比，该类只包括 D1 一个级别，D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。整个计算机系统是不可信任的，硬件和操作系统很容易被侵袭。D1 级计算机系统标准规定对用户没有验证，也就是任何人都可以使用该计算机系统而不会有任何障碍。系

统不要求用户进行登记(要求用户提供用户名)或口令保护(要求用户提供唯一字符串来进行访问)，任何人都可以坐在计算机前并开始使用它。

D1 级的计算机系统包括：DOS、Windows 3.xe 及 Windows 95(不在工作组方式中)；Apple 的 System7.x。

2. C 类安全等级

C 类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。

1) C1 级

C1 又称为选择性安全保护(Discretionary Security Protection)系统，可信任运算基础体制(Trusted Computing Base，TCB)通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C1 级系统要求硬件有一定的安全机制(如硬件带锁装置和需要钥匙才能使用计算机等)，用户在使用前必须登录到系统。C1 级系统还要求具有完全访问控制的能力。C1 级防护不足之处在于用户直接访问操作系统的根。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统的数据任意移走。

常见的 C1 级兼容计算机系统有：UNIX 系统、XENIX、Novell 3.x 或更高版本、Windows NT。

2) C2 级

C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

C2 级在 C1 级的某些不足之处加强了几个特性，C2 级引进了受控访问环境(用户权限级别)的增强特性。这一特性不仅以用户权限为基础，还进一步限制了用户执行某些系统指令。授权分级使系统管理员能够分用户分组，授予他们访问某些程序的权限或访问分级目录。另一方面，用户权限以个人为单位授权用户对某一程序所在目录的访问。如果其他程序和数据也在同一目录下，用户也将自动得到访问这些信息的权限。C2 级系统还采用了系统审计。审计特性跟踪所有的“安全事件”，如登录(成功和失败的)以及系统管理员的工作，如改变用户访问和口令。

常见的 C2 级操作系统有：UNIX 系统、XENIX、Novell 3.x 或更高版本、Windows NT、Windows 2000 和 Windows 2003 等。

3. B 类安全等级

B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B 类安全等级可分为 B1、B2 和 B3 三类。

1) B1 级

B1 级又称为标志安全保护(Labeled Security Protection)，它支持多级安全，对网络、应用程序和工作站等实施不同的安全策略。这种安全级别的计算机系统一般用于政府机构，例如

国防部和国家安全局的计算机系统。

2) B2 级

B2 级别称为结构化的保护(Structured Protection)。B2 级安全要求计算机系统中所有对象加标签，而且给设备(如工作站、终端和磁盘驱动器)分配安全级别。如用户可以访问一台工作站，但可能不允许访问装有人员工资资料的磁盘子系统。B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。

3) B3 级

B3 级，即安全域级别(Security Domain)，必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员，B3 级要求用户工作站或终端通过可信任途径连接网络系统，这一级必须采用硬件来保护安全系统的存储区。

4. A 类安全等级

这是橙皮书中的最高安全级别，这一级有时也被称为验证设计(Verified Design)级别。与前面提到的各级级别一样，这一级包括了它下面各级的所有特性。A 级还附加一个安全系统受监视的设计要求，合格的安全个体必须分析并通过这一设计。另外，必须采用严格的形式化方法来证明该系统的安全性。而且在 A 级，所有构成系统的部件的来源必须安全保证，这些安全措施还必须担保在销售过程中这些部件不受损害。

1) A1 级

A1 级与 B3 级相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。

2) 超 A1 级

超 A1 级在 A1 级基础上增加了许多安全措施，超出了目前的技术发展，这些只是为了今后的工作提供指导，在未来随着更多更先进的分析技术的出现，此级的要求也会变得更加明确清晰。在这一级，设计环境将变得更重要，形式化高层规约的分析将对测试提供帮助。超 A1 级系统涉及的范围包括系统体系结构、安全测试、形式化规约与验证、可信设计环境等。

在网络的具体设计过程中，根据实际情况综合考虑，确定一个比较合理且性能较高的网络安全级别。需要说明的是，TCSEC 标准也存在不足，它只针对孤立的计算机系统，特别是小型机和主机系统；它假设有一定的物理保障，所以该标准适合政府和军队，不一定适合企业用户。因此，各个国家和地区根据不同情况，相继又制定出了不同的安全评价标准。

15.3.3　欧洲的安全评价标准(ITSEC)

在信息安全保障阶段，欧洲四国(英、法、德、荷)提出了评价满足保密性、完整性、可用性要求的《信息技术安全评价准则》(ITSEC，*Information Technology Security Evaluation*

Criteria)，又称欧洲白皮书。ITSEC 除了吸收 TCSEC 的成功经验之外，首次提出了信息安全的保密性、完整性、可用性，把可信计算机的概念提高到了可信信息技术的高度。

ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级。1～5 级对应于 TCSEC 的 D 到 A。F6 至 F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。评估准则分为 6 级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应以及设计与源码在形式上一致。

15.3.4　加拿大的评价标准(CTCPEC)

加拿大 1988 年制定的《加拿大可信计算机产品评估准则》CTCPEC(*Canadian Trusted Computer Product Evaluation Criteria*)专门针对政府需求而设计。1989 年 5 月公布第一版，并于 1993 年 1 月在结合 TCSEC 与 ITSEC 的基础上，公布了第三版。与 ITSEC 类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为四大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类，来表示安全性上的差别，分级条数为 0~5 级。

15.3.5　美国联邦准则(FC)

1993 年，美国对 TCSEC 做了补充和修改，制定了《信息技术安全性评价联邦准则》FC(*Federal Criteria*)，是对 TCSEC 的升级，并引入了“保护轮廓”(PP)的概念。每个轮廓都包括功能、开发保证和评价三部分。FC 充分吸取了 ITSEC 和 CTCPEC 的优点，在美国的政府、民间和商业领域得到广泛应用。

15.3.6　国际通用标准(CC)

1993 年 6 月，CTCPEC、FC、TCSEC、ITSEC 的发起者联合起来，将各自独立的标准组合成一个单一的、能被广泛使用的 IT 安全准则：CC(Common Criteria)。并把结果作为国际标准提交给 ISO，它是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996 年 6 月，CC 第一版发布；1998 年 5 月，CC 第二版发布；1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC，并充分突出了“保护轮廓”概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 共 7 个等级。每一级均需评估 7 个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

1998 年，CC 已经成为事实上的美国安全评估标准。TCSEC 在评估完最后一个产品之后，于 2000 年被废弃。同时，原来使用的 ITSEC 的欧洲国家也停止了该标准的项目，但是旧的程序的某些残余仍然存在。

15.3.7　中国的安全标准

由公安部提出并组织制定、国家质量技术监督局发布的强制性国家标准：《计算机信息

系统安全保护等级划分准则 GB 17859—1999》，将计算机信息系统的安全保护等级划分为五个等级。

第一级：用户自主保护级；

第二级：系统审计保护级；

第三级：安全标记保护级；

第四级：结构化保护级；

第五级：访问验证保护级。

标准适用于对计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。用户可以根据自己计算机信息系统的重要程度确定相应的安全保护级别，并针对相应级别进行建设。

1. 用户自主保护级

本级的计算机信息系统可信计算机通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

1) 自主访问控制

计算机信息系统可信计算机定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。

2) 身份鉴别

计算机信息系统可信计算机初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如：口令)来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。

3) 数据完整性

计算机信息系统可信计算机通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

2. 系统审计保护级

与用户自主保护级相比，本级的计算机信息系统可信计算机实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

1) 自主访问控制

计算机信息系统可信计算机定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息，并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。

2) 身份鉴别

计算机信息系统可信计算机初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算机能够使用户对自己的行为负责。计算机信息系统可

信计算机还具备将身份标识与该用户所有可审计行为相关联的能力。

3) 客体重用

在计算机信息系统可信计算机的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

4) 审计

计算机信息系统可信计算机能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。计算机信息系统可信计算机能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间；删除客体；由操作员、系统管理员或系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含的来源；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。

对不能由计算机信息系统可信计算机独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算机独立分辨的审计记录。

5) 数据完整性

计算机信息系统可信计算机通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

3. 安全标记保护级

本级的计算机信息系统可信计算机具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

1) 自主访问控制

计算机信息系统可信计算机定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息，并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。阻止非授权用户读取敏感信息。

2) 强制访问控制

计算机信息系统可信计算机对所有主体及其所控制的客体(例如：进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算机支持两种或两种以上成分组成的安全级。

3) 标记

计算机信息系统可信计算机应维护与主体及其控制的存储客体(例如：进程、文件、段、设备)相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算机向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算机审计。

4) 身份鉴别

计算机信息系统可信计算机初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算机维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算机使用这些数据鉴别用户身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算机能够使用用户对自己的行为负责。计算机信息系统可信计算机还具备将身份标识与该用户所有可审计行为相关联的能力。

5) 客体重用

在计算机信息系统可信计算机的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

6) 审计

计算机信息系统可信计算机能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

对不能由计算机信息系统可信计算机独立分辨的审计事件，审计机制提供的审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算机独立分辨的审计记录。

7) 数据完整性

计算机信息系统可信计算机通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4. 结构化保护级

本级的计算机信息系统可信计算机建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算机必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算机的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

1) 自主访问控制

计算机信息系统可信计算机定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户和(或)以用户组的身份规定并控制客体的共享；阻止非授用户读取敏感信息，并控制访问权限扩散。

自主访问控制机制根据用户指定的方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。

2) 强制访问控制

计算机信息系统可信计算机对外部主体能够直接或间接访问的所有资源(例如：主体、存储客体和输入输出资源)实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算机支持两种或两种以上成分组成的安全级。

3) 标记

计算机信息系统可信计算机维护与可被外部主体直接或间接访问到的计算机信息系统资源(例如：主体、存储客体、只读存储器)相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算机向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算机审计。

4) 身份鉴别

计算机信息系统可信计算机初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算机维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算机使用这些数据鉴别用户身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算机能够使用户对自己的行为负责。计算机信息系统可信计算机还具备将身份标识与该用户所有可审计行为相关联的能力。

5) 客体重用

在计算机信息系统可信计算机的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

6) 审计

计算机信息系统可信计算机能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间；删除客体；由操作员、系统管理员或系统安全管理员实施的动作，以及其他与系统安全有关的事件。

对不能由计算机信息系统可信计算机独立分辨的审计事件，审计机制提供的审计记录接口可由授权主体调用。这些审计记录区别于计算机信息系统可信计算机独立分辨的审计记录。

计算机信息系统可信计算机能够审计利用隐蔽存储信道时可能被使用的事件。

7) 数据完整性

计算机信息系统可信计算机通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

8) 隐蔽信道分析

系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

9) 可信路径

对用户的初始登录和鉴别，计算机信息系统可信计算机在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

5. 访问验证保护级

本级的计算机信息系统可信计算机满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算机在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；

扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

1) 自主访问控制

计算机信息系统可信计算机定义并控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户和(或)以用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息，并控制访问权限扩散。

自主访问控制机制根据用户指定的方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。访问控制能够为每个命名客体指定命名用户和用户组，并规定他们对客体的访问模式。没有存取权的用户只允许由授权用户指定对客体的访问权。

2) 强制访问控制

计算机信息系统可信计算机对外部主体能够直接或间接访问的所有资源实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。计算机信息系统可信计算机支持两种或两种以上成分组成的安全级。

3) 标记

计算机信息系统可信计算机维护与可被外部主体直接或间接访问到的计算机信息系统资源(例如：主体、存储客体、只读存储器)相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，计算机信息系统可信计算机向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算机审计。

4) 身份鉴别

计算机信息系统可信计算机初始执行时，首先要求用户标识自己的身份，而且，计算机信息系统可信计算机维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统可信计算机使用这些数据，鉴别用户身份，并使用保护机制(例如：口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识，计算机信息系统可信计算机能够使用户对自己的行为负责。计算机信息系统可信计算机还具备将身份标识与该用户所有可审计行为相关联的能力。

5) 客体重用

在计算机信息系统可信计算机的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

6) 审计

计算机信息系统可信计算机能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

对不能由计算机信息系统可信计算机独立分辨的审计事件，审计机制提供的审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算机独立分辨的审计记录。计算机信息系统可信计算机能够审计利用隐蔽存储信道时可能被使用的事件。

7) 数据完整性

计算机信息系统可信计算机通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

8) 隐蔽信道分析

系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

9) 可信路径

对用户的初始登录和鉴别，计算机信息系统可信计算机在它与用户之间提供可信通信路径。该路径上的通信只能由该用户或计算机信息系统可信计算机激活，且在逻辑上与其他路径上的通信相隔离，并能正确加以区分。

10) 可信恢复

计算机信息系统可信计算机提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

公安部负责人表示，实行安全等级保护制度后，将有利于提高公安机关对计算机网络信息系统安全保护的监督管理水平。有关网络安全管理方面的内容，我们将在后面的章节里详细探讨。

本 章 小 结

从 20 世纪 80 年代早期开始，国际计算机安全组织就开始了开发 IT 产品和系统的安全评估方法和标准。第一个被广泛使用的著名的评估标准是《可信计算机系统评估准则》(TCSEC)，尽管它被广泛使用了近 20 年，但是它存在一些缺陷，如局限性、评估过程问题、安全保障和功能的绑定、评估结果缺乏国际通用性、选择需求的不灵活性等。为了解决这些问题，各国安全组织了研究人员不断开发新的评估标准和方法。在这些新的方法中，最著名的是欧洲的信息技术安全评估标准(ITSEC)、加拿大的可信计算机产品评估标准(CTCPEC)以及美国的联邦标准(FC)，这些方法的出现促使了当前得到全球支持的通用标准 CC 的形成。

本章讲述了信息安全评估相关的内容，包括：评估的步骤，需要重点考虑的因素，评估的分类，国际系统安全评估标准，包括著名的橘皮书 TCSEC、ITSEC、CTCPEC、FC、国际通用准则 CC 以及中国公安部制定的安全标准。希望通过学习可以给读者对国际信息安全评估及相关标准有一个清晰的、总体的认识。

课 后 练 习

一、填空题

1. 评估的分类可以分成三种，它们是(　　　　　　)、(　　　　　　)、(　　　　　　)。

2. 风险评估的主要任务有(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)。

3. 两种被安全标准广泛参考吸收其优点的标准，是(　　　　　　)、(　　　　　　)。

4. 在 TCSEC 中，Windows 2003 被划分在(　　　　　　)安全级别中，Unix 属于(　　　　　　)安全级别，Windows 95 的安全级别属于(　　　　　　)级。

5. 在 TCSEC 标准中，安全级别由高到低分别是(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)、(　　　　　　)。

二、选择题

1. TCSEC(Trusted Computer System Evaluation Criteria)，俗称(　　)。
   A. 蓝皮书　　B. 橘皮书　　C. 黄皮书　　D. 红宝书
2. TCSEC 标准将计算机系统的安全划分为(　　)个类别，(　　)个级别。
   A. 4　　B. 5　　C. 6　　D. 8
3. 下述选项中，(　　)是综合了 TCSEC 和 ITSEC 的优点而制定的安全标准。
   A. FC　　B. CC　　C. CTCPEC　　D. IPSec
4. 下述安全标准中，(　　)是目前的国际通用安全标准。
   A. FC　　B. CC　　C. ITSEC　　D. TCSEC
5. 下列操作系统中，属于 TCSEC 的 C 类安全级别的有(　　)
   A. Windows 95　　B. UNIX　　C. Windows NT　　D. Apple Sys 7.x

三、 简答题

1. 安全进行评估的意义是什么？你认为评估的困难是什么？
2. 简述评估的步骤和应考虑的因素。
3. 评估可以分为哪几类？简要描述各类评估的特点。
4. 简述 TCSEC 安全标准的主要内容。
5. 简述中国信息系统安全标准的主要内容。

第16章　计算机网络安全管理

信息网络已经成为维持社会经济活动和生产活动的主要基础资源，成为政治、经济、文化、军事乃至社会任何领域的基础。网络安全管理是信息管理体系中的一个重要环节，本章将结合国内外计算机网络信息安全管理的现状，讨论安全管理的重要性，介绍有关网络安全管理的主要概念，以及有关安全管理标准和相关立法内容。

本章重点

- 概述
- 安全管理标准
- 安全立法

16.1　计算机网络安全管理概述

所谓管理，是指在群体活动当中，为了完成一定的任务，实现既定的目标，针对特定的对象，遵循确定的原则，按照规定的程序，运用恰当的方法，所进行的制订计划、建立相关机构、落实措施、进行培训、检查效果和实施改进等一系列活动。其中，管理的任务、目标、对象、原则、程序和方法是管理策略的内容，一系列的管理活动是在管理策略的指导下进行的。所以，首先要明确管理策略，然后才是开展管理活动。

安全管理是以管理对象的安全为任务和目标的管理。安全管理的任务是保证管理对象的安全。安全管理的目标是达到管理对象所需的安全级别，将风险控制在可以接受的程度。

网络信息安全管理作为企业或组织完整的信息管理体系中的一个重要环节，是以网络信息系统为对象的安全管理。对组织的管理者来说，必须认识到信息管理是一个系统工程，它需要对信息系统的各个环节进行统一的综合考虑、规划和架构，并要兼顾组织内外不断发生的变化，任何环节上的安全疏忽都会对系统构成威胁。

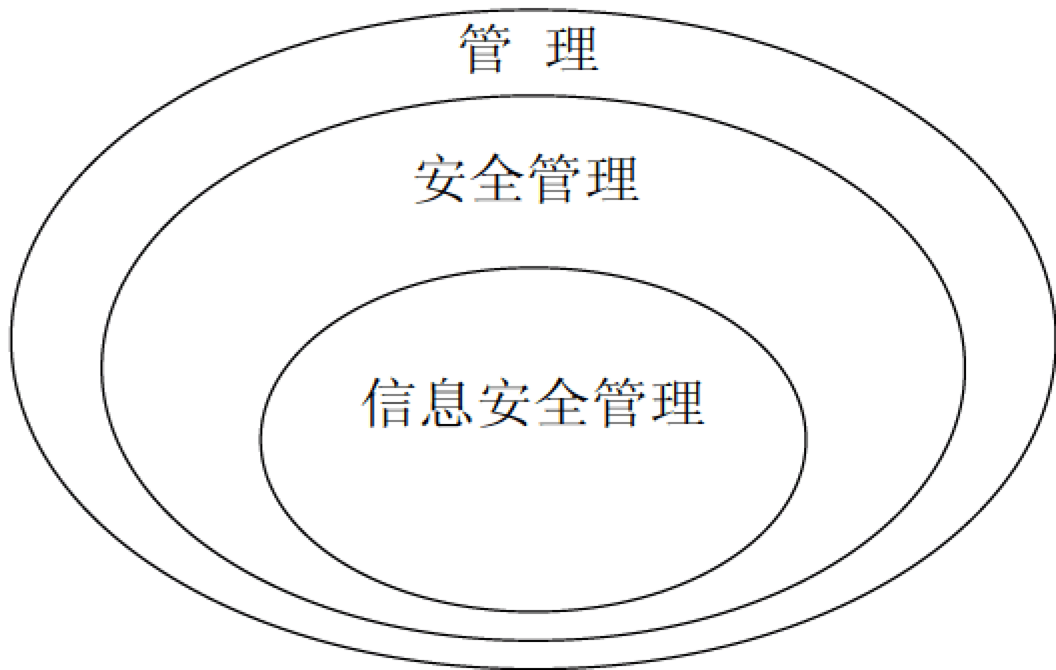


图 16-1　管理、安全管理、网络信息安全管理的关系

图 16-1 描述了管理、安全管理和网络信息安全管理的关系。

16.1.1　网络安全管理的重要性

对网络信息系统不断增强的依赖性使得信息技术在提供工作效率的同时，也增大了重要的信息受到非法侵扰和破坏的可能性，严重的还会面临资产损失、服务中断的情况。当今的网络信息系统既面临着计算机欺诈、商业情报窃取、阴谋破坏、天灾人祸等安全威胁，又面临着像计算机病毒、黑客非法入侵攻击等破坏，而且随着信息技术的迅速发展和应用的深入，各种安全问题也变得越来越错综复杂。

自 1987 年以来，全世界已经发现超过 50 000 种计算机病毒，1999 年 4 月 26 日，中国台湾散布出来的 CIH 病毒大爆发，据不完全统计大陆受其影响的 PC 总数达 36 万台之多；2000 年 5 月爆发的“爱虫”病毒给全球用户造成了数以 100 亿美元计的损失。据 2002 年统计，黑客事件平均每天发生 614 次。Internet 上已经有几万个黑客网站，并且技术不断更新，各种攻击手段达到上千种之多。即便是戒备森严的美国国防部信息系统也遭受过几十万次的黑客攻击，且成功率高达惊人的 63%。历史上还有一些悬而未决的网络犯罪悬案，至今尚无法侦破，具体情况见第 2 章的相关内容。

然而，对计算机网络系统造成最大损失的风险主要还是来自于内部，国际上统计结果表明，企业信息受到的损失中，70%是由于内部员工的疏忽或有意泄露机密造成的。在日益成为国家经济运作的重要支柱的数字化、网络化信息社会中，如果没有信息安全，国家的经济体制和社会安全，金融与货币安全，产业与市场安全，战略物资与能源安全，对外贸易与投资安全就不能得到有效保障。

16.1.2　网络安全管理的内容

信息网络安全管理模型的设计，并没有一个严格统一的标准，不同领域不同时期，人们对信息安全的认识都不尽相同，对解决信息网络安全问题的侧重点也有所不同。从安全管理的发展历程和实施安全管理过程中所使用的方法上，可以分为早期的静态的信息网络安全管理和后期的动态的信息安全管理。

1. 静态的信息安全管理

早在 1989 年，ISO 组织就发布了一个 ISO 7498—2 标准，即《信息处理系统——开放系统互联》，这个标准提供了安全服务与相关体制的一般描述，确定在信息网络安全管理中可以提供这些服务与机制的位置。在其被引入到中国之后，形成了后来的 GB/T 9387.2-1995 标准。ISO 7498—2 标准充分体现了早期的信息网络时期人们对信息安全体系的关注焦点，即以防护技术为主的、静态的信息安全管理体系。

ISO 7498—2 安全管理体系结构由 5 类安全服务及用来支持这些安全服务的 8 种安全机制组成。安全服务体现了安全体系所包含的主要功能及内容，是能够定位某种威胁的安全措施，而安全机制则规定了与安全需求相对应的可以实现安全服务的技术手段。一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；同时，一种安全机制可以提供一种或者多种安全服务。安全服务和安全机制有机结合、相互交叉，在安全体系的不同层次发挥作用。除了 OSI 七层协议中的第五层(会话层)外，其他各层都能够提供相应的

安全服务。ISO 7498—2 这种安全体系充分体现了信息安全层次性和结构性的特点。

ISO 7498—2 定义的安全服务包括如下内容。

- 认证(Authentication 包括实体认证，来源认证)
- 访问控制(Access Control)
- 数据保密性(Data Confidentiality)
- 数据完整性(Data Integrity)
- 抗抵赖性(Non-repudiation)

上述安全服务可以通过以下安全机制来实现。

- 加密机制(Encipherment)
- 数字签名(Digital Signature)
- 访问控制机制(Access Control Mechanisms)
- 认证交换(Authenticatin Exchanges)
- 业务流填充(Traffic Padding)
- 路由控制(Routing Control)
- 公证(Notarisation)

ISO 7498—2 安全体系结构师针对基于 OSI 参考模型的网络通信系统，它所定义的安全服务也只是解决网络通信安全性的技术措施，其他信息安全相关领域，包括系统安全、物理安全、人员安全等方面都没有涉及。这种体系关注的是一种静态的防护技术，它并没有考虑到信息安全动态性和周期性的发展特点，缺乏检测、响应和恢复这些重要的环节，因此无法满足日益复杂更加全面的信息安全保障的要求，从而促使了新的安全体系结构的诞生，后续出现的 PDRR 模型和 PPDR 等动态的信息网络安全体系模型，详见第 2 章的相关内容，在此不再赘述。

2. 动态的信息安全管理

第 2 章介绍过的动态信息安全模型(PPDR)中，安全管理是一个动态的过程，在一定的安全策略的原则下，通过安全防护(P)、安全检测(D)、安全响应(R)等不断循环的动态过程，使安全防护得到不断提高和完善。

信息安全发展至今，人们逐渐已经认识到了安全管理的重要性。在这方面，英国的 BS 7799 标准是一个很好的例子。与以往的以技术为主的安全体系不同，BS 7799 提出的 PDCA 信息安全管理模型是一个系统化、程序化和文档化的管理体系。这其中，技术措施只是作为依据安全需求有选择有侧重地实现安全目标的手段而已。

BS 7799—2 所采用的过程模式如图 16-2 所示，“计划—实施—检查—行动”这四个步骤贯穿整个过程。与前面介绍过的 PDRR 和 PPDR 类似，PDCA 四个英文字母分别表示在 PDCA 循环过程中所代表的四个步骤的英文首字母如下。

- P(Plan)：计划，确定方针和目标，确定活动计划。
- D(Do)：实施，实现计划中的任务。
- C(Check)：检查，总结执行计划的结果，注意效果，找出问题。

● A(Action)：行动，对总结检查的结果进行处理，成功的经验加以肯定并适当推广，将其标准化；失败的教训加以总结，避免重犯；未解决的问题放到下一个 PDCA 循环。

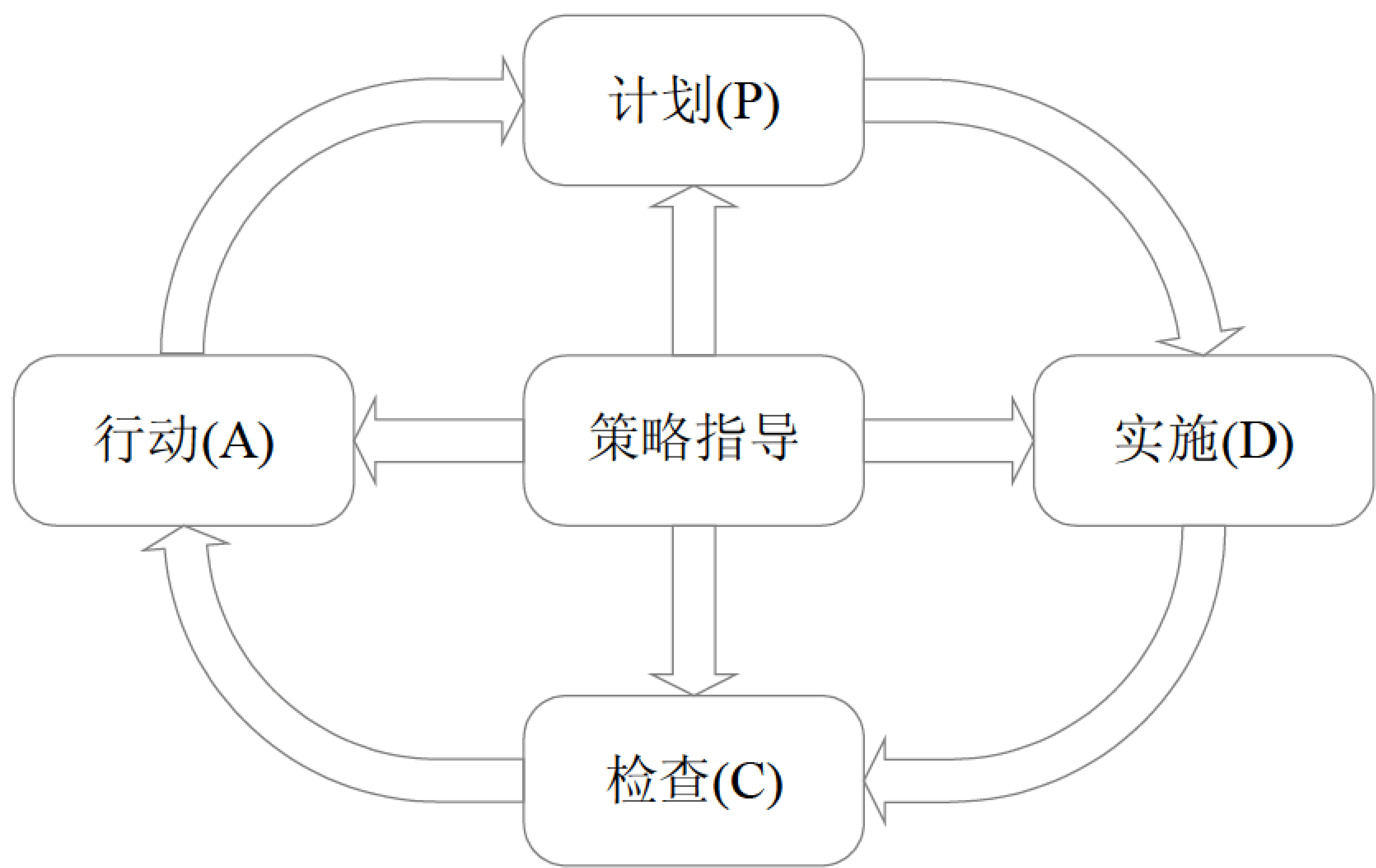


图 16-2　PDCA 过程模式

这四个阶段的具体内容如下。

1) 计划阶段

本阶段的主要任务是根据风险评估、法律法规要求、组织业务运营自身要求来确定控制目标和控制方式。为了确保正确建立信息安全管理体系的范围和内容，识别并评估所有的信息安全风险，为这些风险制订适当的处理计划。策划阶段的所有重要活动都要被文件化，以备将来追溯和控制更改记录。在计划阶段需要完成以下几个工作。

● 确定信息安全方针。
● 确定信息安全管理系统的范围。
● 制订风险识别和评估计划。
● 制订风险控制计划。

2) 实施阶段

这个阶段的主要任务是实施组织所选择的控制目标与控制措施，具体有以下工作。

(1) 风险治理

对被评估认为是可接受的风险，不需要采取进一步的措施；对于不可接受风险，需要实施所选择的控制或转移，这应该与计划阶段中准备的风险处理计划同步进行。

(2) 保证资源、提供培训、提高安全意识

这个阶段需要分配适当的资源(人员、时间和资金)，运行信息安全管理体系以及所有的安全控制。

提高信息安全意识的目的就是产生适当的风险和安全文化，保证意识和控制活动的同步，还必须安排针对信息安全意识的培训，并检查意识培训的效果，以确保其持续有效和实时性。

3) 检查阶段

检查阶段是 PDCA 循环的关键阶段。本阶段的主要任务是进行有关方针、程序、标准与法律法规的检查，目的是保证控制措施有效进行。

4) 行动阶段

本阶段的主要任务是对信息安全管理体系进行评价，寻求改进的机会，采取相应的措施。为了使信息安全管理体系持续有效，应以检查阶段采集的不符合项信息为基础，经常进行调整与改进。对信息安全管理体系所做的改变或下一步行动计划，要及时通知所有的相关部门，并提供相应的培训。

16.1.3　网络安全管理的原则

网络安全管理的原则是一组规则，定义了一个组织要实现的安全目标和实现这些安全目标的途径。信息安全管理的内容应该有别于技术方案，信息安全原则只是描述一个组织保证信息安全的途径的指导性纲领，它不涉及具体做什么和如何做的问题，只指出要完成的目标任务。原则性的规则不涉及具体实现细节，对于整个组织提供全局性指导，为具体的安全措施和规定提供一个全局性的框架。

常用的信息网络安全管理原则有如下几种。

- 加密原则——描述组织对数据加密的安全要求。
- 使用原则——描述设备使用、计算机服务使用和雇员安全规定，以保护组织的信息和资源安全。
- 线路连接原则——描述诸如传真发送和接收、模拟线路与计算机连接、拨号连接等安全要求。
- 反病毒原则——给出有效减少病毒对组织的威胁的一些指导方针，明确在哪些环节必须进行病毒检测。
- 应用服务提供原则——定义应用服务提供者必须遵守的安全方针。
- 审计原则——描述信息审计要求，包括审计小组的组成、权限、事故调查、安全风险评估、信息安全符合程度评价、对用户和系统活动进行监控等活动的要求。
- 电子邮件使用原则——描述组织内部和外部电子邮件接收、传递的安全要求。
- 数据库原则——描述存储、检索、更新等管理数据库数据的安全要求。
- 非武装区域原则——定义位于“非军事区域”的设备和网络分区。
- 第三方的连接原则——定义第三方接入的安全要求。
- 敏感信息原则——描述组织的机密信息分级，按照它们的敏感程度描述安全要求。
- 内部活动原则——描述组织内部的各种活动安全要求，使组织的产品服务和利益受到充分保护。
- Internet 接入原则——定义在组织防火墙之外的设备和操作的安全要求。
- 口令防护原则——定义创建、保护和改变口令的要求。
- 远程访问原则——定义从外部主机或网络连接到组织的网络进行外部访问的安全要求。
- 路由器安全原则——定义组织内部路由器和交换机的最低安全配置。
- 服务器安全原则——定义组织内部服务器的最低安全配置。

- VPN 安全原则——定义通过 VPN 接入的安全要求。
- 无线通讯原则——定义无线系统接入的安全要求。

16.2　安全管理标准

发达国家非常重视制订信息安全发展战略和计划，美、俄、日国家都已经或者已经制订出自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。2000 年初，美国出台了电脑空间安全计划，旨在加强关键基础设施、计算机系统和网络免受威胁的防御能力。2000 年 9 月 12 日，俄罗斯批准了《国家信息安全构想》，明确保护信息安全应采取的措施。我国还没有制定国家级别的信息安全战略，但是在“十五”规划中已经提及。另外，在我国 2001 年度的《高科技研究发展计划》中提出了信息安全的科研攻关课题。“863”计划信息安全技术发展战略研究专家制订了《信息安全技术应急计划》。

目前国际上制定了大量的有关信息安全的国际标准，主要可分为互操作标准、技术与工程标准、信息安全管理与控制标准。

常见的信息管理与控制标准有以下几个。

1. 信息安全管理标准(ISO/IEC 13335)

《IT 安全管理方针》系列已经在国际社会中开发了很多年。几个组成部分分别为：ISO/IEC13335-1：1996《IT 安全的概念与模型》、ISO/IEC13335-2：1997《IT 安全管理和计划制定》、ISO/IEC13335-3：1998《IT 安全管理技术》、ISO/IEC13335-4：2000《安全措施的选择》、ISO/IEC13335-5：《网络安全管理方针》。

2. 信息安全管理体系标准(BS7799，其中一部分成为 ISO/IEC 17799)

BS—7799 是由英国标准协会(British Standards Institution，简称 BSI)制定的信息安全管理体系标准，BS—7799 为保障信息的机密性、完整性和可用性提供了典范。它包括两部分，其中第一部分《信息安全管理实施规则》于 2000 年 12 月被国际化标准组织(ISO)纳入世界标准，编号为 ISO/IEC 17799。BS—7799 广泛地覆盖了所有的信息安全议题，如安全方针的制定、安全责任的归属、风险的评估、定义与强化安全参数及访问控制，甚至包含防病毒的相关策略等。BS—7799 已经成为国际公认的信息安全实施标准，适用于各种产业与组织。

16.2.1　ISO 27000

ISO 为信息安全管理体系标准预留了 ISO/IEC 27000 系列编号，类似于质量管理体系的 IS 9000 系列和环境管理体系的 ISO 14000 系列标准。

信息安全管理体系(Information security management systems，简称 ISMS，即 ISO/IEC27000 系列)是目前国际信息安全管理标准研究的重点。ISO 27000 系列共包括 10 个标准，当前已经发布和在研究的有 6 个，分别如下。

(1) ISO27000 原理与术语 PrinciplesandVocabulary。

(2) ISO27001 信息安全管理体系——要求 ISMS Requirements(以 BS7799—2 为基础)。

(3) ISO27002 信息技术安全技术信息安全管理实践规范(ISO/IEC17799：2005)。

(4) ISO27003 信息安全管理体系——风险管理 ISMSRisk Management。

(5) ISO27004 信息安全管理体系——指标与测量 ISMSMetricsand Measurement。

(6) ISO27005 信息安全管理体系——实施指南 ISMSImplementation Guidelines。

ISO 27000 标准对应用于信息安全管理体系的 ISO/IEC 27000 系列标准的概况、状态和关系提供说明，并规定了与 ISO/IEC 27000 ISMS 系列标准相关的术语。ISO/IEC 27000 标准有三个章节，第一章是标准的范围说明，第二章对 ISO 27000 系列的各个标准进行了介绍，说明了各个标准之间的关系，包括 ISO 27000、ISO 27001、ISO 27002、ISO 27003、ISO 27004、ISO 27005、ISO 27006。第三章给出了与 ISO 27000 系列标准相关的术语和定义，共 63 个。

16.2.2　ISO 27001

ISO 27001 是 ISO 27000 系列的主标准，类似于 ISO 9000 系列中的 ISO 9001，各类组织可以按照 ISO 27001 的要求建立自己的信息安全管理体系(ISMS)，并通过认证。该标准源于 BS 7799—2，主要提出 ISMS 的基本要求，已于 2005 年 10 月正式发布。在正式版发布之前一段时期，有效的标准是 BS7799—2：2002。当 ISO 27001 正式发布后，BS 7799—2：2002 被撤销。

ISO 27001 用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系(Information Security Management System，ISMS)提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织的 ISMS 的设计和实施受业务需求和目标、安全需求、所采用的过程以及组织的规模和结构的影响。上述因素及其支持过程会不断发生变化。期望信息安全管理体系可以根据组织的需求而测量，例如简单的情形可采用简单的ISMS 解决方案。ISO 27001 标准可以作为评估组织满足顾客、组织本身及法律法规的信息安全要求的能力的依据，无论是组织自我评估还是评估供方能力，都可以采用，也可以用作独立第三方认证的依据。

16.2.3　ISO 27002

ISO 27002 标准取代 ISO /IEC 27002：2005 ，直接由 ISO/IEC 27002：2005 更改标准编号为 ISO/IEC 27002。

ISO 27002 标准为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。ISO 27002 标准概述的目标提供了有关信息安全管理通常公认的目标的通用指南。标准的控制目标和控制措施预期被实施以满足由风险评估所识别的要求。此标准可以作为一个实践指南服务于开发组织的安全标准和有效的安全管理实践，帮助构建组织间活动的信心。ISO 27002 标准包含的实施规则可以认为是开发组织具体指南的起点。实施规则中的控制和指导并不全都是适用的。而且，可能需要本标准中未包括的附加控制和指南。当开发包括附加控制和指南的文件时，包括对该标准适用的条款进行交叉引用可能是有用的，该交叉引用便于审核员和商业伙伴进行符合性核查。

16.3 安全立法

网络犯罪对法学研究产生了深远影响，它不仅仅对法学理论和现行法律体系、法律规定带来了冲击也为法学理论的全球化和法律规定的趋同及司法协助带来了新的契机。

网络立法是建立和完善法律体系的需要，是调整网络犯罪所引起的社会冲突问题的需要，是保障网络健康发展的需要，是使人们懂得维护自己权益、同网络犯罪作斗争的需要，也是教育人守法、预防犯罪的需要。

16.3.1 国际安全法律法规

以法律的形式制定和规范信息安全工作，是有效实施安全措施的最有力保证。制定网络信息安全规则的开路先锋是各大门户网站，美国的雅虎和美国在线等网站都在实践中形成了一套自己的信息安全管理方法。美国和欧洲共同体是计算机网络安全比较完善的国家和组织，一些发展中国家和第三世界国家的计算机网络安全方面的法规还不够健全。

2000 年 10 月 1 日，美国电子签名法正式生效。2000 年 10 月 5 日，美国参议院通过了《互联网网络完备性及关键设备保护法案》。2000 年 9 月，俄罗斯实施了关于网络信息安全的法律。欧洲共同体是一个在欧洲范围内具有较强影响力的政府间组织。为在共同体内正常地进行信息市场运作，该组织在诸多问题上建立了一系列的法律，具体包括：《竞争(反托拉斯)法》、《产品责任、商标和广告规定法》、《知识产权保护法》、《保护软件、数据和多媒体产品及在线版权法》以及《数据保护法》、《跨境电子贸易法》、《税收法》、《司法》等。这些法律若与其成员国原有国家法律相矛盾，则必须以共同体的法律为准。可见，欧洲共同体制定的法律效用凌驾于成员国各自的原有法律之上。

互联网上的犯罪现象有一个突出的特点就是它的国际化，网络犯罪是一种国际化的犯罪，它危害到了整个世界的网络安全。因此世界各国应该联合起来进行广泛的合作和研讨，像打击国际恐怖组织一样打击网络犯罪。一方面，国际社会已经制定了相应的制裁网络犯罪的国际公约，世界各发达国家也已经制定了各国的反网络犯罪的法律。另一方面，许多发展中国家却因为网络的不普及，而忽视了相关方面的法律的制定。这一状况给予网络罪犯生存的空间。只有全世界都行动起来，让各国法律相互接轨，形成一个严密的国际法律合作体系，才能有效地打击国际网络犯罪。因此，我国从一开始制定相关的网络安全立法，就注重与国际法律体系和惯例接轨，以避免在实际运用中所产生的国际摩擦和冲突。

16.3.2 国内安全法律法规

1994 年 2 月 18 日，中华人民共和国国务院令 147 号发布《中华人民共和国计算机信息系统安全保护条例》。随后陆续出台了一些关于计算机系统和网络的行政法规，1997 年 12 月 11 日国务院批准 1997 年 12 月 30 日公安部发布了《计算机信息网络国际联网安全保护管理办法》，同年在新修订的《刑法》中，新增了一些条款，直接规定了信息安全犯罪的问题。2001 年，九届全国人大通过了《全国人民代表大会常务委员会关于维护互联网安全的决定》，并已开始起草《计算机网络与信息安全管理条例》等行政法规。截止到 2002 年，我国正式颁

布的信息安全相关国家标准已达几十项，其中包括《中华人民共和国安全法》、《中华人民共和国保守国家秘密法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国商用密码保护条例》等。国家公安部、国家安全部、国家保密局、国家密码管理委员会等相继制定、颁布了一批信息安全的行业标准。

1. 中华人民共和国计算机信息系统安全保护条例

《中华人民共和国计算机信息系统安全保护条例》的内容如下。

1) 总则

(1) 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

(2) 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

(3) 计算机信息系统的安全保护应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

(4) 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

(5) 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。

(6) 公安部主管全国计算机信息系统安全保护工作。

国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

(7) 任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

2) 安全保护制度

(1) 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

(2) 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

(3) 计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。

(4) 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

(5) 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

(6) 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

(7) 对计算机信息系统中发生的案件，有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

(8) 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

(9) 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

3) 安全监督

(1) 公安机关对计算机信息系统安全保护工作行使下列监督职权。

- 监督、检查、指导计算机信息系统安全保护工作。
- 查处危害计算机信息系统安全的违法犯罪案件。
- 履行计算机信息系统安全保护工作的其他监督职责。

(2) 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

(3) 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

4) 法律责任

(1) 违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

- 违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；
- 违反计算机信息系统国际联网备案制度的；
- 不按照规定时间报告计算机信息系统中发生的案件的；
- 接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；
- 有危害计算机信息系统安全的其他行为的。

(2) 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

(3) 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

(4) 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15 000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

(5) 违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚法》的有关规定处罚；构成犯罪的，依法追究刑事责任。

(6) 任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

(7) 当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

(8) 执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

5) 附则

(1) 本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

(2) 军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

(3) 公安部可以根据本条例制定实施办法。

(4) 本办法自发布之日起施行。

2. 计算机信息网络国际联网安全保护管理办法

《计算机信息网络国际联网安全保护管理办法》的具体条例如下。

1) 总则

(1) 为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定，制定本办法。

(2) 中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

(3) 公安部计算机管理监察机构负责计算机信息国际联网的安全保管管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

(4) 任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

(5) 任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息。

- 煽动抗拒、破坏宪法和法律、行政法规实施的。
- 煽动颠覆国家政权，推翻社会主义制度的。
- 煽动分裂国家、破坏国家统一的。
- 煽动民族仇恨、民族歧视，破坏民族团结的。
- 捏造或者歪曲事实，散布谣言，扰乱社会秩序的。
- 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪。
- 公然侮辱他人或者捏造事实诽谤他人的。
- 损害国家机关信誉的。
- 其他违反宪法和法律、行政法规的。

(6) 任何单位和个人不得从事下列危害计算机信息网络安全的活动。

- 未经允许，进入计算机信息网络或者使用计算机信息网络资源的。
- 未经允许，对计算机信息网络功能进行删除、修改或者增加的。
- 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的。
- 故意制作、传播计算机病毒等破坏性程序的。
- 其他危害计算机信息网络安全的。

(7) 用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

2) 安全保护责任

(1) 从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

(2) 国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

(3) 互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责。

- 负责本网络的安全保护管理工作，建立健全安全保护管理制度。
- 落实安全保护技术措施，保障本网络的运行安全和信息安全。
- 负责对本网络用户的安全教育和培训。
- 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核。
- 建立计算机信息网络电子公告系统的用户登记和信息管理制度。
- 发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告。
- 按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

(4) 用户在接入单位办理入网手续时，应填写用户备案表。备案表由公安部监制。

(5) 互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

(6) 使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

(7) 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

3) 安全监督

(1) 省、自治区、直辖市公安厅(局)、地(市)、县(市)公安局，应当有相应机构负责国际联网的安全保护管理工作。

(2) 公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

(3) 公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安

全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

(4) 公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

(5) 公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

4) 法律责任

(1) 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，按照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

(2) 有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

- 未建立安全保护管理制度。
- 未采取安全技术保护措施的。
- 未对网络用户进行安全教育和培训的。
- 未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的。
- 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的。
- 未建立电子公告系统的用户登记和信息管理制度的。
- 未建立公用账号使用登记制度的。
- 转借、转让用户账号的。

(3) 违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

(4) 违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

5) 附则

(1) 与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

(2) 办法自发布之日起施行。

本 章 小 结

本章主要讨论了有关网络安全管理的概念和重要性，描述了几种不同分类的网络安全管理标准，如静态的安全管理和动态的信息安全管理，并对它们进行分析比较。然后，介绍了国际上制定的一些有关信息安全管理标准，包括 ISO/IEC 13335、ISO/IEC 17799、ISO/IEC27000、ISO/IEC27001、ISO/IEC27002。最后，结合国际上相关的网络安全管理法例，介绍了中国自己制定的相关安全立法，着重介绍了《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》的内容，使读者对网络安全管理有一个整体的认识，旨在能够让读者接受、理解相关的管理标准，并将相关的标准运用到实际工作当中，有章可循、有法可依，更好更有效地实施安全防护措施，确保网络信息安全、稳定、可靠，满足不同层次网络安全的需求。

课 后 练 习

一、填空题

1. 从网络安全管理过程中所使用的方法来看，分为(　　　　　)、(　　　　　)两种。

2. 静态的网络安全管理，相对后期的动态管理模式而言，缺少(　　　　　)、(　　　　　)、(　　　　　)几种安全防范的环节。

3. PDCA 安全管理模型中，四个主要的环节是(　　　　　)、(　　　　　)、(　　　　　)、(　　　　　)。

4. ISO 27000 系列共包括(　　　　　)个标准，当前已经发布和在研究的有(　　　　　)个。

5. 本章介绍的中国相关网络安全法规分别是(　　　　　)、(　　　　　)。

二、选择题

1. ISO 7498—2 定义的安全服务包括(　　)。

A. 数据保密性　　B. 访问控制　　C. 加密机制　　D. 认证

2. PDCA 安全管理模型的四个步骤，包括下面的(　　)。

A. 响应　　B. 计划　　C. 恢复　　D. 检查

3. 下述选项中，(　　)属于动态安全管理模式的环节。

A. 响应　　B. 计划　　C. 恢复　　D. 检查

4. 下述的(　　)属于网络安全管理原则的范畴。

A. 加密　　B. 访问控制　　C. 抗抵赖　　D. 认证

5. ISO 27000 标准总共有(　　)个标准，已经发布和在研究的有(　　)个。

A. 6　　B. 8　　C. 10　　D. 7

三、简答题

1. 网络安全管理的重要意义是什么？
2. 简述安全管理的内容和分类，并比较其不同。
3. 安全管理标准可以分为哪几类？简要描述 ISO 27000 系列标准的主要内容。
4. 说一说安全法规制定需要注意哪些问题。
5. 结合第 2 章相关安全模型的内容，说明 PPDR、PDRR 和 PDCA 的特点和不同。